FOR IMMEDIATE RELEASE: Distributable Formal Statement by Jon "GainSec" Gaines, the Independent Security Researcher who discovered, disclosed, conducted the analysis and authored the white paper: *Examining the security posture of an Anti-Crime Ecosystem*

Original Release Date: 11/05/2025
Current Version Release Date: 11/06/2025

Contact for verification or follow-up: whitepaper@gainsecmail.com

DISTRIBUTABLE FORMAL STATEMENT

Disclaimer

This statement documents good faith, independently conducted security research performed exclusively on lawfully acquired hardware under the researcher's control. No testing involved unauthorized access to any network, account, or production environment. All methods complied with 18 U.S.C. § 1030 and 17 U.S.C. § 1201 (g) exemptions for good-faith security testing.

The content is intended to inform defenders and vendors; it is not an instruction manual for exploitation. Replication on systems not under explicit authorization violates U.S. and international computer-misuse law.

The author affirms that this research was performed independently, without financial support, employment, consultancy, or material benefit from the vendor or its affiliates. No funding, compensation, or third-party direction influenced the selection of targets, the methods used, or the interpretation of results. The devices analyzed were purchased by the author. Tests were confined to offline/lab environments; no interception of third-party communications or content prohibited by ECPA/Title III occurred; no human-subjects' data were collected.

The purpose of this study is to advance public understanding of security posture and responsible disclosure practices, not to promote or discredit any product or company. This document, in its current version, is intended for defensive-security evaluation, compliance verification, and policy development. Redistribution that adds operational detail, live credentials, or working exploits is prohibited.

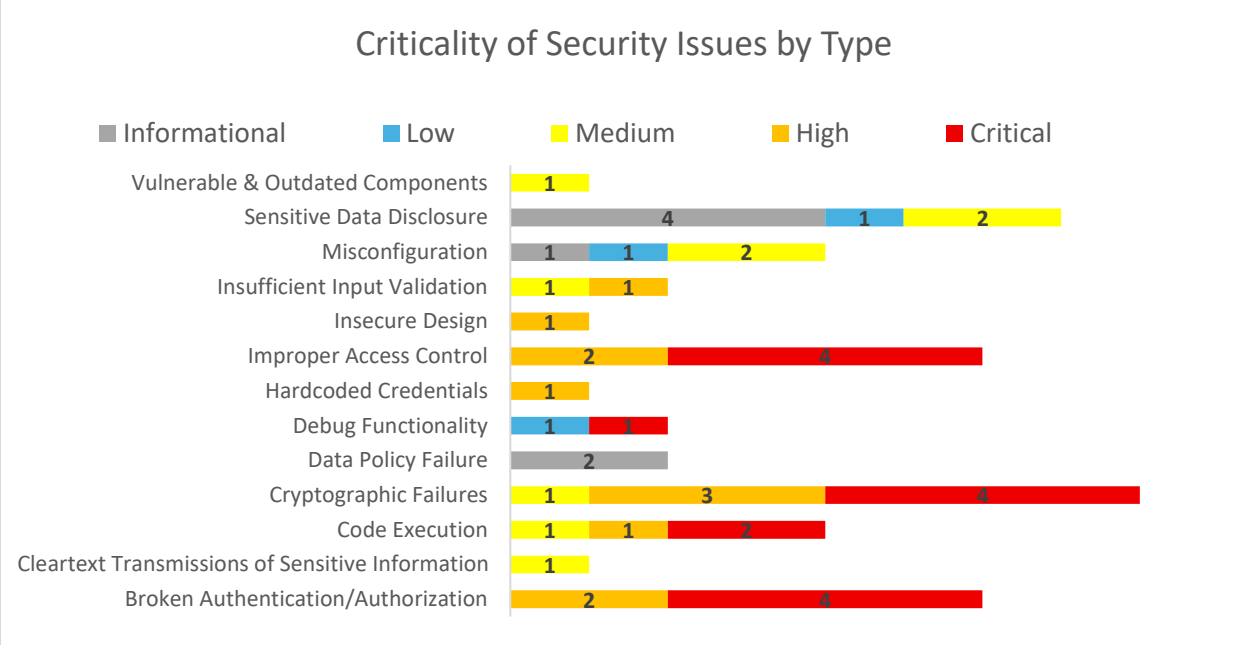
Descriptions omit operational steps and live secrets by design. Any reproduction must be limited to assets the reader owns or is authorized to assess, in controlled labs, and solely to validate remediation. Do not apply to third-party or deployed systems.

Background

I submit this statement as an independent security researcher with over a decade of professional offensive security experience. This statement condenses my whitepaper which consolidated findings from my multipart independent research into Flock Safety's hardware (Raven Gunshot Detection; Falcon/Sparrow/Flex LPR; Bravo Compute Box), the Android applications deployed on those devices as well as those available on public app stores. The work followed responsible disclosure practices and resulted in assigned and pending CVE identifiers via MITRE with the National Vulnerability Database (NVD) program managed by the National Institute of Standards and Technology (NIST) and sponsored by the Department of Homeland Security (DHS).

Summary of Probable Cause

Analysis identified recurring deficiencies in cryptographic enforcement, access control implementation, and key management. Version 1.1-PR of the white paper documents forty-five (45) findings across three device families, shared applications, and publicly available applications; twenty-two (22) carry CVE identifiers, with additional CVEs pending. The Total Findings Chart below substantiate category distribution across devices.



Material Facts

1) Hardware trust chain is disabled at scale. Raven Gunshot Detection System ships without Secure Boot and with flash unencrypted; rollback protection absent (CVE-2025-47819, CVE-2025-47820). LPR units have Secure Boot disabled, bootloader unlocked, EDL/QDL accepting unsigned loaders (CVE-2025-47822) and unencrypted EMMC (CVE-2025-47824). Bravo Compute Box repeats the pattern: Secure Boot off (CVE-2025-59408), bootloader unlocked (CVE-2025-59404), unauthenticated EDL/QDL (CVE-2025-59402), unencrypted UFS.

2) Administrative plane is unauthenticated. The "Collins" service exposes device administration on all Interfaces without authentication, including live view toggling, reboots, log/crashpack retrieval, and enabling ADB over TCP (CVE-2025-59403).

3) Hidden debug enables wireless access with uniform weak credentials. A specific but simple button press sequence starts a device hotspot; default password "<redacted_password>" is uniform across units (CVE-2025-59403).

4) ADB authentication disabled; sideloading permitted. LPR and Bravo allow unauthenticated ADB and APK sideloading, providing trivial code execution footholds when chained with the items above.
5) End of Life operating system in the field. LPR devices run Android Things 8.1 (EOL 2022), violating basic lifecycle controls and increasing exploit exposure.
6) Hardcoded secrets and key material in production. Multiple applications embed API keys, a Java Keystore password used for mTLS, and a static OAuth client secret (e.g., CVE-2025-47823, CVE-2025-59407, CVE-2025-59406).
7) Data policy weaknesses. Retention defaults to capacity thresholding rather than time/event policy; recordings may be written to a public external path without app-level encryption. It remains unclear whether these configurations persist in deployed production units.

Context of Exposure

Devices are commonly mounted on short, publicly accessible poles; physical interfaces remain externally accessible under typical deployment configurations. In the latest iteration, the physical trigger for enabling the hotspot remains exposed, compounding the risk from unauthenticated APIs and ADB. Observed weaknesses permit unauthorized command execution, data exfiltration, and device manipulation through trivially reproducible vectors.

Technical Detainment/Remediation

1) Enforce Secure Boot, lock bootloaders, require authenticated, signed loaders for all EDL/QDL interactions; enable at rest encryption for flash/EMMC/UFS across Raven, LPR, and Bravo.
2) Bind administrative APIs (Collins) to authenticated channels; disable ADB over TCP enablement via HTTP; restrict to loopback or a mutually authenticated control plane.
3) Remove hidden hotspot triggers; replace uniform passwords with per-device credentials; require explicit operator pairing for any debug or service shell.
4) Ship Android apps with ‘android:debuggable=false;’ remove unauthenticated ADB pathways and sideload capability on production builds.
5) Rotate and revoke embedded keys, keystore passwords, OAuth client secrets; issue per-device mTLS materials; eliminate client-side key exposure.
6) Replace capacity only retention with time/event policies; store media in file based encrypted app-private storage or encrypt before externalization.
7) Migrate LPR off End-of-Life OS; establish patch management and inventory capable of immediate decommissioning and SIM revocation where remediation is infeasible.

Declaration & Contact

This declaration is accurate to the best of the researcher’s knowledge and derived from contemporaneous research records.

It is intended for distribution to journalists, privacy advocates, regulators, law enforcement leadership, counsel, and legislators evaluating current deployments and required corrective actions.

This formal statement may be redistributed verbatim for transparency, provided operational details remain redacted. Derivative publication requires preservation of attribution, version number (1.1 PR), and checksum of the signed PDF.

Full Whitepaper is available at https://github.com/gainsec/anti-crime-ecosystem-research
Mirror: https://zenodo.org/records/17529424
White Paper DOI: 10.5281/zenodo.17529424

For further inquiries about this statement or its formal whitepaper, please reach out to the email included at the beginning of this statement.