CVE-2025-21042: Samsung Galaxy Zero-Day Exploited in LANDFALL Spyware Campaign

socradar.io/cve-2025-21042-samsung-galaxy-0day-landfall-spyware

Ameer Owda November 11, 2025

A critical security vulnerability affecting Samsung Galaxy devices, tracked as CVE-2025-21042, has been confirmed as actively exploited and listed in CISA's Known Exploited Vulnerabilities (KEV) Catalog.

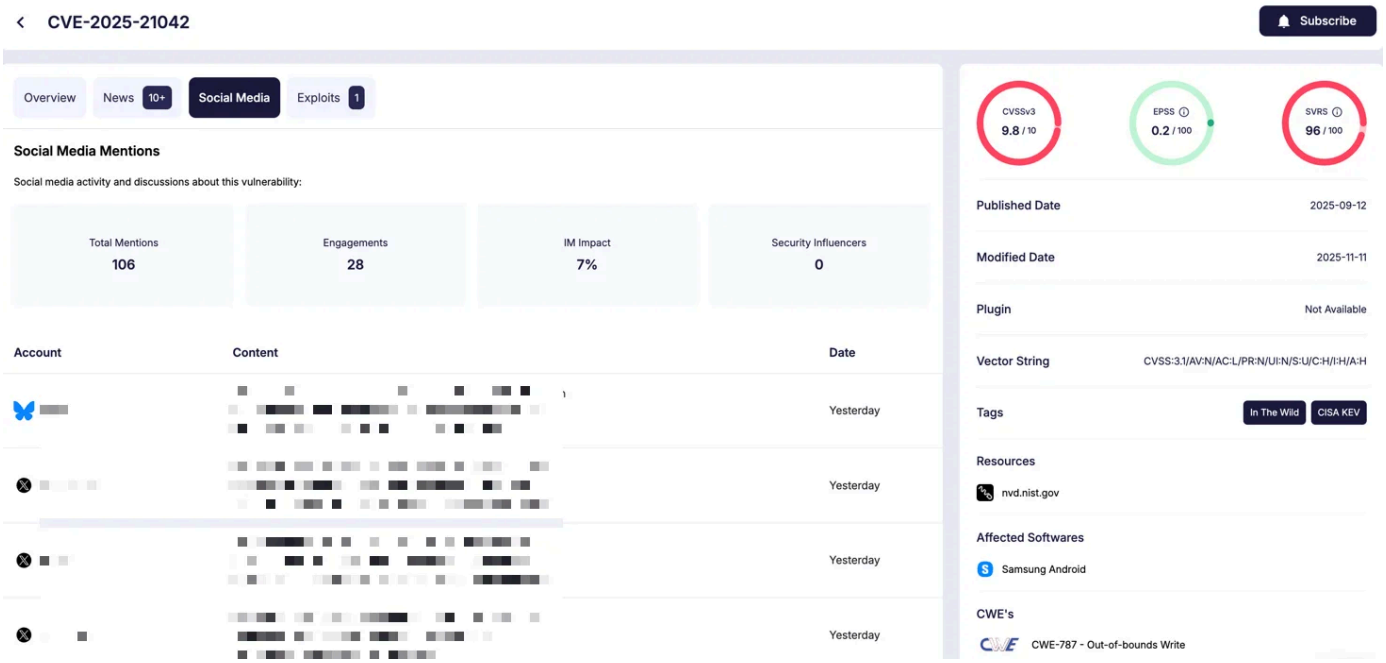
Recently, the vulnerability has been linked to a sophisticated spyware campaign, LANDFALL, which used malicious image files to compromise targeted Samsung Galaxy models through apps such as WhatsApp.

This blog provides a detailed examination of CVE-2025-21042, how the exploitation occurred, which devices were affected, and what mitigations users and organizations should implement.

What Is CVE-2025-21042?

CVE-2025-21042 (CVSS 9.8) is a critical out-of-bounds write vulnerability located in Samsung's **libimagecodec.quram.so** library, responsible for image decoding on Samsung mobile devices.

This flaw allows data to be written outside its intended memory boundaries. The vulnerability is remotely exploitable and can be triggered through a specially crafted image file, allowing Remote Code Execution (RCE) and control over the affected device.



Details of CVE-2025-21042 (SOCRadar Vulnerability Intelligence)

Samsung initially addressed the issue in its April 2025 Security Maintenance Release (SMR). But, the devices that have not installed this update remain vulnerable. Because the flaw resides in a central image library, any application relying on it to process untrusted images may serve as an attack vector.

CISA Adds CVE-2025-21042 to the Known Exploited Vulnerabilities Catalog

CISA has added CVE-2025-21042 to its Known Exploited Vulnerabilities (KEV) catalog following verified reports of active exploitation.

According to CISA's guidance, all Federal Civilian Executive Branch (FCEB) agencies are required to apply Samsung's recommended mitigations or discontinue use of unpatched devices by **December 1, 2025**.

SAMSUNG | MOBILE DEVICES

CVE-2025-21042

Samsung Mobile Devices Out-of-Bounds Write Vulnerability: *Samsung mobile devices contain an out-of-bounds write vulnerability in libimagecodec.quram.so. This vulnerability could allow remote attackers to execute arbitrary code.*

Related CWE: CWE-787

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2025-11-10
- **Due Date:** 2025-12-01

Additional Notes +

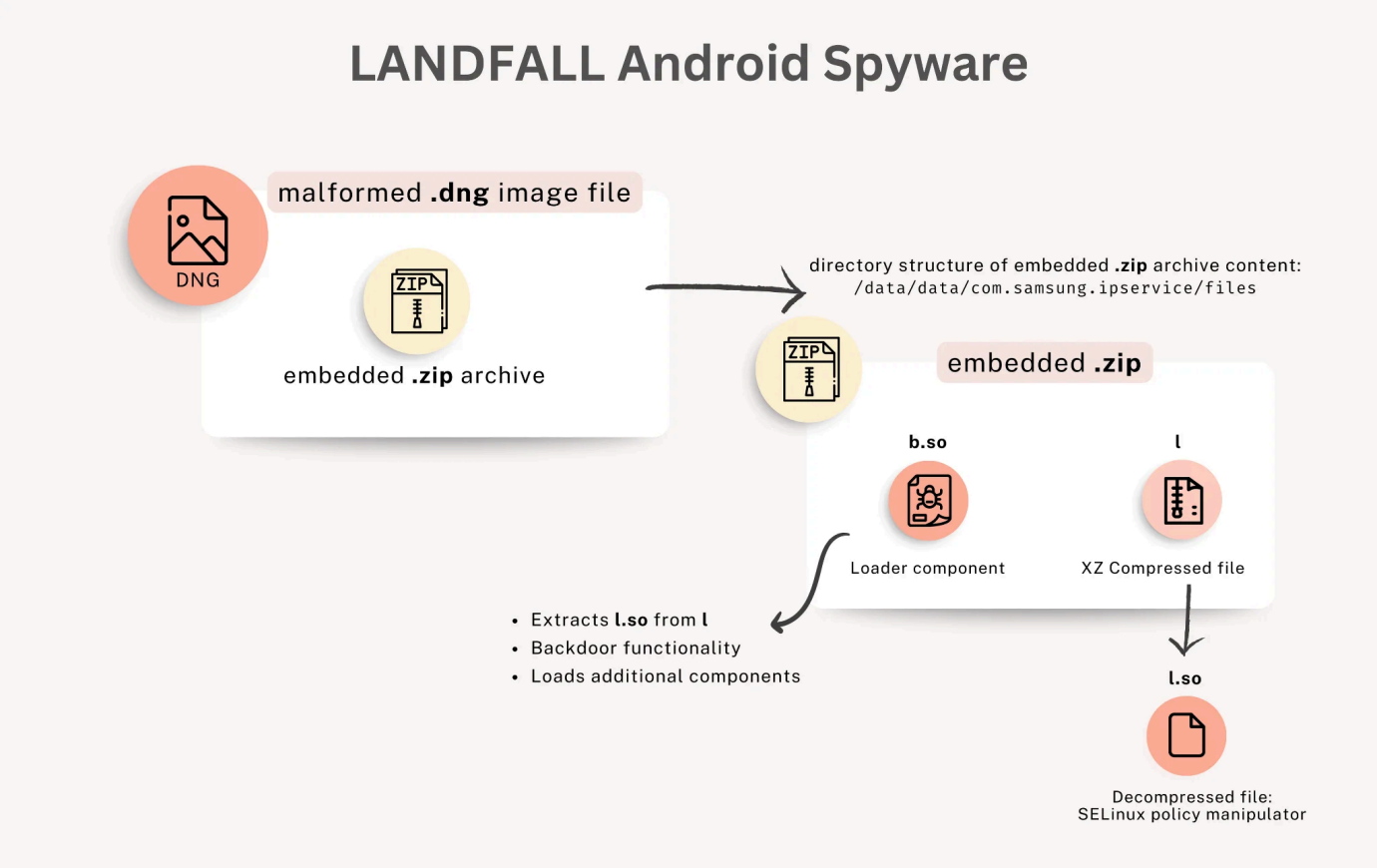
CVE-2025-21042 listed on CISA's KEV catalog

This directive underscores the severity of the flaw and serves as a transition point to examine how the vulnerability was leveraged in the LANDFALL spyware campaign, which revealed the full impact of this exploitation.

How Was CVE-2025-21042 Exploited by the LANDFALL Campaign?

Researchers discovered the **LANDFALL** spyware family, which leveraged CVE-2025-21042 within a complex exploit chain that specifically targeted Samsung Galaxy smartphones.

Attackers crafted **malformed DNG image files** (Digital Negative format) containing an embedded ZIP archive appended to the image data. When a vulnerable device processed these files through libimagecodec.quram.so, the exploit executed and extracted malicious components from the archive, including a loader file named **b.so**, internally referenced as **"Bridge Head."**



How does LANDFALL Android spyware operate? (Unit 42)

Evidence strongly indicates that the spyware spread through **zero-click or near-zero-click delivery via WhatsApp**. VirusTotal samples, labeled with names such as **"WhatsApp Image"** and **WA0000**, appeared between July 2024 and early 2025, confirming exploitation months before public disclosure.

Once installed, LANDFALL granted attackers extensive surveillance capabilities, including audio and call recording, geolocation tracking, photo and message exfiltration, and SELinux policy manipulation for persistence and privilege escalation.

Which Samsung Devices Were Targeted?

The LANDFALL spyware was engineered for flagship Samsung devices. Debug strings within its loader referenced **Galaxy S22**, **S23**, **S24**, **Z Fold4**, and **Z Flip4** models. Telemetry and sample submissions confirm that these flagship models were the primary focus of exploitation efforts.

Regions Affected by the LANDFALL Campaign

Telemetry and VirusTotal sample data suggest that potential targets include **Iraq, Iran, Turkey, and Morocco**, aligning with patterns typical of regional surveillance operations.

Attribution and Infrastructure Insights

Researchers observed that the campaign's infrastructure and methodology mirror those used by commercial spyware vendors operating in the Middle East, although no definitive attribution has been established.

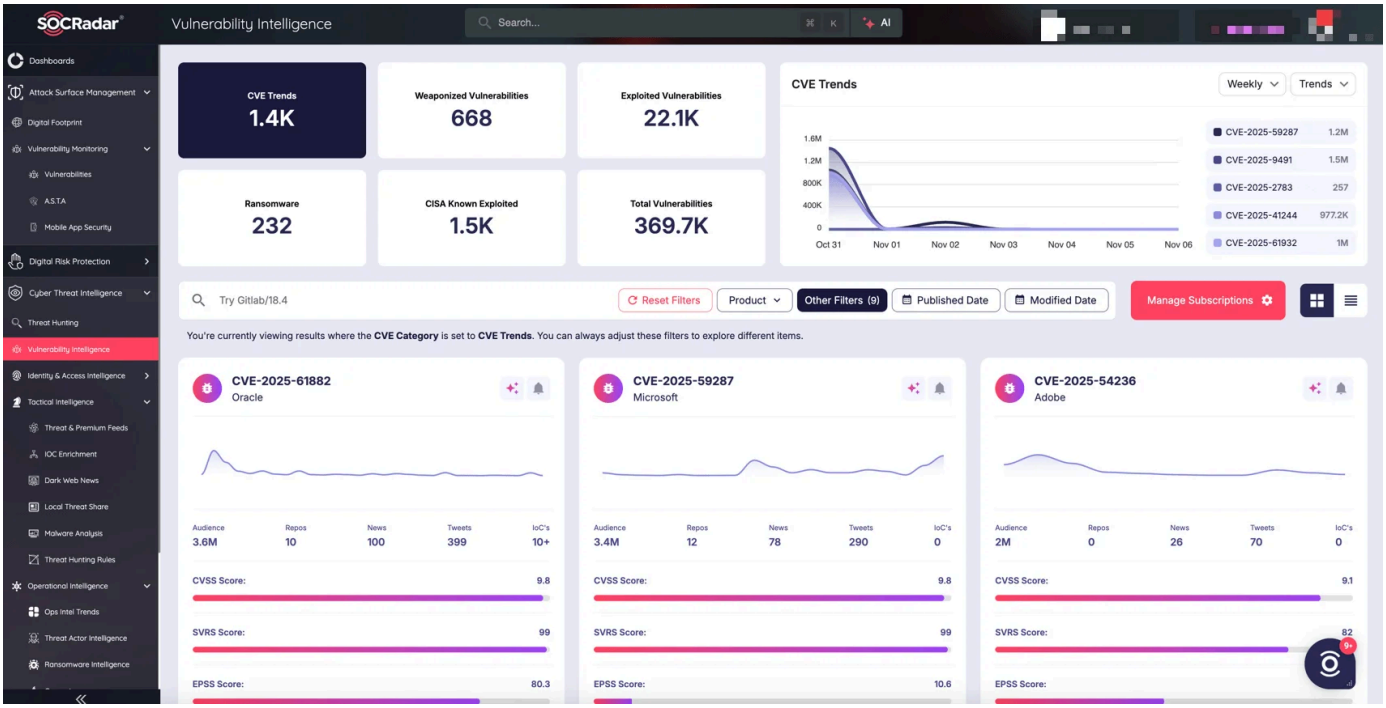
The spyware's Command and Control (C2) infrastructure used deceptive domains hosted on European servers, and activity persisted from mid-2024 through late 2025, reflecting a deliberate, sustained espionage campaign rather than opportunistic attacks.

How Does CVE-2025-21042 Relate to Other Image-Based Mobile Exploits?

CVE-2025-21042 exemplifies an emerging trend in mobile exploitation: targeting **complex media parsers** that automatically handle images in messaging and gallery applications. Between 2024 and 2025, several related vulnerabilities reinforced this pattern:

- Samsung later patched another DNG parsing flaw within the same library (CVE-2025-21043).
- Apple mitigated a separate DNG image processing zero-day (CVE-2025-43300) that attackers combined with a WhatsApp vulnerability (CVE-2025-55177) to compromise iOS devices.

Researchers indicate that DNG-based exploits have become a preferred delivery vector for spyware, given that image files are widely shared and often processed without user interaction.



Track the latest CVEs and exploits with SOCRadar's Vulnerability Intelligence

Gain proactive insight with **SOCRadar's Cyber Threat Intelligence (CTI) module**, designed to keep you ahead of emerging vulnerabilities like CVE-2025-21042. With real-time vulnerability intelligence, exploit tracking, and correlation across global threat feeds, it enables your security team to prioritize patching and mitigate risks faster.

Additionally, integrated **Attack Surface Management (ASM)** capabilities provide continuous visibility into exposed assets, helping you discover, assess, and secure your digital footprint before threat actors strike – all within a unified intelligence platform.

Recommended Mitigations for CVE-2025-21042 on Samsung Android Devices

Although Samsung resolved this vulnerability in April 2025, unpatched devices remain exposed. Users and organizations should implement the following actions:

For individual users:

- **Install the latest firmware.** Navigate to Settings → Software update → Download and install and confirm the device runs the **April 2025 SMR** or newer.
- **Update messaging applications, particularly WhatsApp.** Maintain the latest app versions to ensure all associated security fixes are applied.
- **Disable automatic media downloads** to minimize exposure to malicious image files.
- **Monitor for signs of compromise,** such as abnormal battery consumption, unexpected data transfers, or unfamiliar applications.

For enterprises and government agencies:

- **Enforce patch compliance** through mobile device management (MDM) or unified endpoint management (UEM) platforms. Restrict network access for outdated devices.
- **Follow CISA KEV directives and BOD 22-01 guidance.** Prioritize remediation of all KEV-listed vulnerabilities and align patch timelines with CISA's deadlines.
- **Monitor network traffic** for connections to known LANDFALL Command and Control domains and implement blocking rules as appropriate.
- **Deploy mobile threat defense solutions** to detect suspicious behavior, isolate compromised devices, and collect forensic evidence.

By applying these updates and controls, organizations and users can significantly reduce the risk of exploitation through CVE-2025-21042 and related image-processing vulnerabilities.

Indicators of Compromise (IOCs)

Based on Unit 42's analysis of the LANDFALL spyware campaign exploiting CVE-2025-21042, the following indicators of compromise (IOCs) have been identified. Security teams are advised to monitor for any communication with the listed IP addresses or domains and to block or flag any

file hashes matching these indicators.

Malicious File Hashes (SHA256)

- 9297888746158e38d320b05b27b0032b2cc29231be8990d87bc46f1e06456f93 – WhatsApp Image 2025-02-10 at 4.54.17 PM.jpeg
- b06dec10e8ad0005ebb9da24204c96cb2e297bd8d418bc1c8983d066c0997756 – IMG-20250120-WA0005.jpg
- c0f30c2a2d6f95b57128e78dc0b7180e69315057e62809de1926b75f86516b2e – WhatsApp Image 2024-08-27 at 11.48.40 AM.jpeg
- b975b499baa3119ac5c2b3379306d4e50b9610e9bba3e56de7dfd3927a96032d – PHOTO-2024-08-27-11-48-41.jpg
- 29882a3c426273a7302e852aa77662e168b6d44dcebfca53757e29a9cdf02483 – IMG-20240723-WA0001.jpg
- b45817ffb0355badcc89f2b7d48eecf00ebdf2b966ac986514f9d971f6c57d18 – IMG-20240723-WA0000.jpg

LANDFALL Components

- ffeeb0356abb56c5084756a5ab0a39002832403bca5290bb6d794d14b642ffe2 – b.so component (Bridge Head loader)
- d2fafc7100f33a11089e98b660a85bd479eab761b137cca83b1f6d19629dd3b0 – b.so component
- a62a2400bf93ed84ebadf22b441924f904d3fcda7d1507ba309a4b1801d44495 – b.so component
- 384f073d3d51e0f2e1586b6050af62de886ff448735d963dfc026580096d81bd – b.so component
- 211311468f3673f005031d5f77d4d716e80cbf3c1f0bb1f148f2200920513261 – XZ compressed SELinux policy manipulator
- 69cf56ac6f3888efa7a1306977f431fd1edb369a5fd4591ce37b72b7e01955ee – l.so SELinux policy manipulator (extracted)

Command and Control (C2) Servers

- 194.76.224[.]127 – brightvideodesigns[.]com
- 91.132.92[.]35 – hotelsitereview[.]com
- 92.243.65[.]240 – healthyeatingontherun[.]com
- 192.36.57[.]56 – projectmanagerskills[.]com
- 46.246.28[.]75 – Unknown domain
- 45.155.250[.]158 – Unknown domain