GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

26 November 2025

Advisory 112: Commercial Spyware Targeting Users of Mobile Messaging Applications

Release Date: 25th of November 2025
Impact: HIGH / CRITICAL
TLP: CLEAR

The Department of Communication and Digital Transformation (DCDT through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that utilize the above products. This alert is intended to be understood by technical users and systems administrators.

What is it?

Commercial spyware (also called "commercial-grade" or "surveillance" spyware), refers to off-the-shelf or brokered surveillance tools sold to government or private buyers that can remotely monitor and control mobile devices. Threat actors are using these tools to target messaging app users by compromising accounts and delivering-on malware or persistent monitoring implants that exfiltrate messages, calls, location, media, and other sensitive data.

What are the Systems affected?

Not limited to a single app or OS: These campaigns target users of multiple messaging apps (Signal, WhatsApp, Telegram, etc) on mobile platforms (Android and iOS) and may leverage platform or app vulnerabilities in addition to social engineering

What does this mean?

How attackers exploit this vulnerability (attack vector)

1. **Phishing & malicious QR / device-linking codes:** Attackers send links or QR codes that, when scanned or clicked, link the victim's account to an attacker-controlled device or persuade users to install malicious apps/dropper installers.
2. **Zero-click exploits:** Exploits that require no user interactions (e.g., a specially crafted message or media) can deliver spyware silently and are highly effective for targeted compromise.
3. **Impersonation / trojanized apps:** Attackers create malicious apps or web pages impersonating legitimate messaging platforms to trick victims into installing spyware. Once installed, spyware abuses permissions or platform features to exfiltrate data and spread to contacts.
4. **Follow-on-exploitation:** After initial access to an account or device, attackers deploy additional payloads (credential harvesters, persistent implants, data exfiltration modules) to deepen access and persistence

Mitigation process

CERTVU recommend:

- Immediate update OS and Apps.
- Only install apps from trusted stores.
- Turn on multi-factor / two-step verification
- Do not scan untrusted QR codes / links

Reference

1. https://thehackernews.com/2025/08/whatsapp-issues-emergency-update-for.html
2. https://unit42.paloaltonetworks.com/landfall-is-new-commercial-grade-android-spyware/
3. https://cloud.google.com/blog/topics/threat-intelligence/russia-targeting-signal-messenger/