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 RÉPUBLIQUE DEVANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

SPP 9108 Port-Vila, Vanuatu
Tél: (678) 33380

26 novembre 2025

Avis 112 : Logiciels espions commerciaux ciblant les utilisateurs d'applications de messagerie mobile

Date de publication : 25 novembre 2025
Degré d'impact : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN par l'intermédiaire du CERT Vanuatu (CERTVU)), publie la présente alerte.

Cette alerte s'adresse aux organisations et administrateurs de système/réseau utilisant les produits mentionnés ci-dessus. Elle est destinée à être comprise par des utilisateurs techniques et administrateurs de système.

Objet de l'alerte

Les logiciels espions commerciaux (également appelés logiciels espions « de qualité commerciale » ou « de surveillance ») se rapportent à des outils de surveillance prêts à l'emploi ou négociés, vendus à des acheteurs gouvernementaux ou privés, qui permettent de surveiller et de contrôler à distance des appareils mobiles. Les acteurs malveillants utilisent ces outils pour cibler les utilisateurs d'applications de messagerie en compromettant les comptes et en déployant des logiciels malveillants ou des implants de surveillance persistants qui exfiltrent les messages, les appels, la localisation, les médias et d'autres données sensibles.

Systèmes concernés

Non limitées à une seule application ou à un seul système d'exploitation : ces campagnes ciblent les utilisateurs de plusieurs applications de messagerie (Signal, WhatsApp, Telegram, etc.) sur les plateformes mobiles (Android et iOS) et peuvent exploiter les vulnérabilités des plateformes ou des applications en plus de l'ingénierie sociale.

Implication

Les attaquants peuvent exploiter cette vulnérabilité par les manières suivantes (vecteur d'attaque) :

1. **Hameçonnage et codes QR/codes de liaison d'appareils malveillants :** les attaquants malveillants envoient des liens ou des codes QR qui, lorsqu'ils sont scannés ou consultés, relient le compte de la victime à un appareil contrôlé par l'attaquant ou persuadent les utilisateurs d'installer des applications malveillantes/des programmes d'installation de logiciels malveillants.
2. **Exploits sans clic :** les exploits qui ne nécessitent aucune interaction de la part de l'utilisateur (par exemple, un message ou un média spécialement conçu) peuvent diffuser des logiciels espions discrètement et sont très efficaces pour compromettre des cibles spécifiques.
3. **Usurpation d'identité / applications trojanisées :** les attaquants malveillants créent des applications ou des pages Web malveillantes qui usurpent l'identité de plateformes de messagerie légitimes afin d'inciter les victimes à installer des logiciels espions. Une fois installés, ces logiciels espions abusent des autorisations ou des fonctionnalités de la plateforme pour exfiltrer des données et se propager aux contacts.
4. **Suivi de l'exploitation :** après avoir accédé initialement à un compte ou à un appareil, les attaquants déploient des charges utiles supplémentaires (collecteurs d'identifiants, implants persistants, modules d'exfiltration de données) pour approfondir leur accès et leur persistance.

Mesures d’atténuation

Le CERTVU recommande les mesures suivantes :

- Mise à jour immédiate du système d'exploitation et des applications.
- Installation d'applications provenant uniquement de boutiques fiables.
- Activation de la vérification multifactorielle / en deux étapes.
- Interdiction de scanner des codes QR / liens non fiables.

Références

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/