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 DE VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

SERVICE DE COMMUNICATION ET DE TRANSFORMATION NUMÉRIQUE

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

1er septembre 2025

Avis 96 :
Date de publication : 30 août 2025
Degré d'impact : ÉLEVÉ/ CRITIQUE
TLP : CLAIR

CERT Vanuatu (CERTVU) et le service de Communication et de Transformation numérique (SCTN) publient la présente alerte

Cette alerte concerne les organisations et les personnes utilisant les services google, en particulier Gmail. Elle est destinée à tous les utilisateurs en ligne de Google et Gmail, ainsi qu'aux administrateurs de système.

Objet de l'alerte

CERTVU souhaite vous faire part de l'information qui suit :

En juin 2025, des acteurs malveillants appartenant à une entité connue sous le nom d'UNC6040 (également active sous le nom de ShinyHunters) ont réussi à infiltrer l'un des systèmes Salesforce de l'entreprise Google. Ce système contenait les coordonnées professionnelles et les notes de vente des petites et moyennes entreprises. Bien qu'aucun mot de passe Gmail ou Google Drive ni aucune information financière n'aient été divulgués, cette infraction a augmenté la vulnérabilité face aux campagnes de phishing ciblées qui utilisent les données de contact compromises.

Systèmes concernés

- Le conflit ne concerne pas les services aux consommateurs, ce qui signifie que Gmail et d'autres produits destinés aux utilisateurs finaux ont été directement victimes d'infractions.
- Cependant, les données issues de l'infraction de Salesforce sont désormais utilisées pour lancer des attaques de phishing (par e-mail) visant les utilisateurs de Gmail.

Implication

- Les attaquants ont mis au point des campagnes convaincantes, se faisant passer pour des employés de Google ou du support informatique afin d'inciter les utilisateurs à réinitialiser leurs mots de passe et à divulguer leurs codes 2FA.
- Appels d'hameçonnage vocaux (vishing) provenant de numéros de téléphone et d'indicatifs régionaux légitimes, aboutissant éventuellement à la prise de possession de comptes.
- Le risque que ShinyHunters intensifie ses tactiques en créant un site de fuite de données ou en se livrant à des campagnes d'extorsion à l'aide des coordonnées volées ne cesse de croître.

Mesures d'atténuation

CERTVU conseille à tous les utilisateurs de Google/Gmail de sécuriser leurs comptes Gmail contre les menaces en cours et recommande vivement les précautions suivantes :

- Modifiez sans tarder votre mot de passe Gmail.
- Activer l'authentification à deux facteurs (2FA).
- Rester vigilant face aux tentatives d'hameçonnage et de vishing.

Références

1. https://cybersecuritynews.com/gmail-users-password-reset/?fbclid=IwY2xjawMhxyNleHRuA2FlbQIxMABicmlkETFvV1ZRYmNpNk1ZNnFCSmk3AR50Cx4of2J_jWdg25cGrq0xI-D1mtFTfYyKvEL5zmxKTl324iqCnC81yw4-iQ_aem_WtQYJ2E3zRWd8rrMiCZr9Q
2. https://news.trendmicro.com/2025/08/26/google-data-breach-gmail/