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

23 Disemba 2025

Advaes namba 110: Vulnerabiliti long saed blong *Out-of-Bounds Write* blong *WatchGuard Firebox*

Deit we hemi rilis:	12 Novemba 2025
Impak:	HAE / KRITIKOL
TLP:	KLIA

Dipatmen blong Komunikesen mo Dijitol Transfomesen (DKDT) tru long CERT Vanuatu (CERTVU), i givimaot advaeseri ia.

Woning ia hem i blong olgeta Oganaesesen mo Sistem/Netwok Administreta we oli yusum prodak ia. Woning ia oli mekem blong olgeta teknikol yusa mo sistem administreta oli andastanem.

Wanem ia?

CVE-2025-9242 – hem i wan *out-of-bound write* wiknes o vulnerabiliti insaed long *IKEv2 daemon* blong *WatchGuard Firewall OS*. Wan rimot ataka we i no nidim otoraesesen, bae save eksploitem wiknes o vulnerabiliti ia blong eksekutum *arbitrary code* long divaes ia.

Hemia i afektem wanem Sistem?

Hem i afektem:

- Firewall OS Versions 11.10.2 kasem 11.12.4_update1, 12.0 kasem 12.11.13 mo 2025.1
- Vulnerabiliti ia i impaktem espeseli ol konfigaresen taem oli yusum divaes blong:
    1. VPN blong Mobael Yusa we i stap yusum IKEv2
    2. Brans Ofis VPN IKEv2 *with a dynamic gateway peer*

Hemia i minim wanem?

Olsem wanem ol ataka oli eksploitem vulnerabiliti ia (atak vekta)

- Ataka i tagetem IKEv2 VPN seves (espeseli hemia we oli save kasem long netwok baondri) mo i kosem wiknes ia tru long wan spesifik IKE AUTH o *certificate payload* we oli krietem we i kosem *buffer write* blong ran bitim nomol taem blong hem.
- Eksekusen i hapen bifo long *authentication* (i.e., ataka i no nidim valid pas blong login) blong oli save tekem kontrol long divaes taem hem i ekspos long ekstenol trafik.
- Taem ataka i tekem kontrol long aplaens, hem i save pivot i go insaed long intenol netwok, distebem VPN trafik, instolem ol bakdoa, o fasilitetem wok blong transferemaot data witaot otoraesesen / *ransomware*. From se aplaens ia hem i stap long netwok baondri, bae i gat posibiliti se ataka i tekem kontrol long ful netwok.

Proses blong Katem Daon Risk

CERTVU i rikomendem se:

Mekem pajing kwiktaem – Aplaem paj blong venda we oli rilisim:

- Blong 12.x brans: apgreid i go long vesen **12.11.4** (o semak vesen we oli fiksim)
- Blong 2025.1 brans: apgreid i go long **2025.1.1** (o wan vesen we i moa hae)
- Not: No dipen o trastem ol *end-of-life* vesen (olsem 11.x brans) blong sekiuriti we i stap gohed.

Sipos pajing i no save tekem ples kwiktaem:

- Limitim IKEv2/UDP 500 mo UDP 4500 akses long ol *endpoints* nomo we oli trastem.
- Disebolem ol VPN konfiguresen we oli no yusum (espeseli ol *dynamic gateway peer setups*).
- Monitarem ol indiketa blong eksploitesen: Large IKE_AUTH payload.

Refrens

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://www.cve.org/CVERecord?id=CVE-2025-9242