

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



GOVERNEMENT 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

24 Septemba 2025

Advaes namba 99: CVE-2024-40766 – Vulnerabiliti long saed blong SonicOS Akses Kontrol we i no propa.

Deit we hemi rilis: 10 Septemba 2025

Impak: HAE / KRITIKOL

TLP: KLIA

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

Woning ia hemi blong olgeta Oganaesesen mo Sistem/Netwok Administreta we oli yusum olgeta prodak antap ia. Olgeta teknikal yusa mo sistem administreta bae oli mas andastanem woning ia.

CERTVU i save long inkris long aktiv eksploitesen blong vulnerabiliti ia we i kamap long 2024 olsem wan kritikol vulnerabiliti insaed long *SonicWall SSL VPNs*.

Wanem ia?

Vulnerabiliti ia hem i wan akses kontrol we i no propa mo oli faenem insaed long *SonicWall SonicOS* manejen akses mo SSLVPN, mo bae save lid i go long olgeta risos akses we oli no otoraesem, mo long ol spesifik kondisen hem i mekem *firewall* i krash.

Hemia i afektem wanem Sistem?

Vulnerabiliti ia i afektem ol *SonicWall Gen 5* mo *Gen 6* divaes mo ol *Gen 7* divaes we oli stap ranem *SonicOS 7.0.1-5035* mo ol olfala vesen.

[Yu save go long link ia blong luk diteil blong ol vesen we oli etails of infected versions can view viewed here](#)

Hemia i minim wanem?

Olsem wanem nao bae ol ataka oli eksploitem wiknes o vulnerabiliti ia:

1. Akses we oli no otoraesem tru long ol Akses Kontrol we i no propa –Vulnerabiliti ia i mekem ol ataka -witaot verifikesen – oli faenem wei araon blong aksesem ol kontrol mo kasem akses we oli no otoraesem.
2. *Ransomware Deployment (Notably Akira)* – Taem oli stap insaed tru long SSL VBN akses we oli go raon long hem, ol ataka – espeseli olgeta afiliet blong *Akira ransomware* – oli yusum entri poen ia blong lonjem *ransomware* o rimuvum ol data.

Proses blong Katem Daon Risk

1. Apgreid mo aplae niufala paj blong olgeta vesen we hem i afektem.
[Go long link ia blong luk ol diteil](#) blong Sekiuriti Advaes blong CVE-2024-40766.
2. Paswod apdeit blong ol Lokol Yusa – *SonicWall* i mekem strong rikomendesen se evri yusa blong ol Gen5 mo Gen6 *firewalls* wetem ol SSLVPN akaon we oli manejem lokoli oli mas apdeitem paswod blong olgeta kwiktaem blong impruvum sekiuriti mo stopem akses we oli no otoraesem.

Ridim moa abaot Gen7 mo ol niu SonicWall Firewalls = SSLVPN risk aktiviti.

Refrens

1. <https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015>
2. cisa.gov/known-exploited-vulnerabilities-catalog