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

17 décembre 2025

Avis 115 : Vulnérabilité Fortinet_CVE-2025-59718 -CVE-2025-59719

Date de publication : 9 décembre 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

- **CVE-2025-59718** : cette vulnérabilité concerne une vérification incorrecte des signatures cryptographiques dans certaines versions de Fortinet FortiOS, FortiProxy et FortiSwitchManager, qui pourrait permettre à un attaquant non authentifié de contourner l'authentification de connexion FortiCloud SSO via un message de réponse SAML spécialement conçu.

- **CVE-2025-59719** : cette vulnérabilité concerne une vérification incorrecte des signatures cryptographiques dans Fortinet FortiWeb, qui pourrait permettre à un attaquant non authentifié de contourner l'authentification de connexion FortiCloud SSO via un message de réponse SAML spécialement conçu.

Systèmes concernés

Versions affectées :

FortiOS: 7.0.0–7.0.17, 7.2.0–7.2.11, 7.4.0–7.4.8, 7.6.0–7.6.3

FortiProxy: 7.0.0–7.0.21, 7.2.0–7.2.14, 7.4.0–7.4.10, 7.6.0–7.6.3

FortiSwitchManager: 7.0.0–7.0.5, 7.2.0–7.2.6

FortiWeb: 7.4.0–7.4.9, 7.6.0–7.6.4, 8.0.0

Implication

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

- Compromission administrative totale des appareils Fortinet.
- Modifications de configuration, création de nouveaux comptes administrateur ou désactivation des contrôles de sécurité.
- Mouvement latéral plus profond dans le réseau de l'entreprise.

Mesures d’atténuation

Le CERTVU recommande les mesures suivantes :

- Appliquez immédiatement les derniers correctifs de Fortinet sur tous les produits concernés.
- Désactivez la connexion SSO FortiCloud sur les appareils jusqu'à ce qu'ils soient corrigés.
- Vérifiez les appareils pour détecter tout signe d'accès non autorisé, de nouveaux comptes ou de modifications de configuration inattendues.
- Limitez l'accès à l'interface de gestion aux adresses IP de confiance ou à l'accès VPN uniquement.
- Consultez l'avis de sécurité des produits Fortinet pour obtenir des informations détaillées sur les mises à jour et les mesures d'atténuation.

Références

1. https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/critical-vulnerabilities-in-multiple-fortinet-products-forticloud-sso-login-authentication-bypass
2. https://fortiguard.fortinet.com/psirt/FG-IR-25-647
3. https://arcticwolf.com/resources/blog/cve-2025-59718-and-cve-2025-59719/
4. https://thehackernews.com/2025/12/fortinet-ivanti-and-sap-issue-urgent.html