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

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

1er juin 2026

Avis 142 : Vulnérabilité Fortinet FortiAuthenticator

Date de publication : 12 mai 2026
Degré d'implication : ÉLEVÉ / CRITIQUE
TLP : CLAIR

Le service de Communication et de Transformation numérique (SCTN), par l'intermédiaire du CERTVU publie l'avis suivant.

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

Objet de l'alerte

CVE-2026-44277 est une vulnérabilité critique (CVSS 9.8) affectant Fortinet FortiAuthenticator. La faille est classée comme une vulnérabilité de contrôle d'accès inadéquat (CWE-284).

Systèmes concernés

Les versions suivantes de Fortinet FortiAuthenticator sont affectées :

- FortiAuthenticator **8.0.0** et **8.0.2**
- FortiAuthenticator **6.6.0 à 6.6.8**
- FortiAuthenticator **6.5.0 à 6.5.6**
- FortiAuthenticator **6.4.0 à 6.4.10**

Implications

La vulnérabilité est **exploitable à distance via le réseau** et peut être utilisée **sans authentification préalable.**

Chaîne d'exploitation typique :

1. **Découverte de la cible**
   - Les attaquants identifient les appliances FortiAuthenticator exposées sur Internet.
2. **Envoi de requêtes spécialement conçues**
   - Des requêtes HTTP/HTTPS malveillantes sont transmises aux services vulnérables ou aux interfaces de gestion.
3. **Contournement du contrôle d'accès**
   - L'appliance valide de manière inadéquate les autorisations d'accès.
4. **Exécution non autorisée de commandes ou de code**
   - L'attaquant exécute des commandes ou interagit avec des fonctionnalités privilégiées.
5. **Activités post-compromission**
   - Les attaquants peuvent :
     - Dérober des données d'authentification
     - Manipuler les flux MFA
     - Créer des comptes non autorisés
     - Effectuer un pivot vers les systèmes internes de l'entreprise

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

- Mettre à niveau vers les versions corrigées :

  - 6.5.7 ou ultérieure
  - 6.6.9 ou ultérieure
  - 8.0.3 ou ultérieure

Références

1. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
2. https://nvd.nist.gov/vuln/detail/CVE-2026-44277
3. https://fortiguard.fortinet.com/psirt/FG-IR-26-128