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

1 June 2026

Avis 140 : CISCO – vulnérabilités liées à la porte dérobée FIRESTARTER (CVE-2025-20333 et CVE-2025-20362).

Date de publication : 23 avril 2026
Degré d'impact : 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

Ces avis portent sur deux vulnérabilités critiques dans les produits de sécurité réseau de Cisco les logiciels Adaptive Security Appliance (ASA) et Firepower Threat Défense (FTD) qui ont été activement exploitées conjointement par un acteur avancé de menace persistante (APT) sophistiqué et soutenu par un État, connu sous le nom de UAT- 4356 (également suivi sous les noms d'ArcaneDoor et Storm-1849).

Ce qui rend cette campagne particulièrement dangereuse est une deuxième étape : même après que les organisations aient corrigé les deux CVE, une porte dérobée spécialement conçue appelée FIRESTARTER peut déjà être intégrée dans l'appareil. Le simple correctif ne la supprime pas. L'acteur malveillant peut continuer à accéder indéfiniment au dispositif compromis, sauf si des mesures supplémentaires spécifiques sont mises en œuvre.

Systèmes concernés

La vulnérabilité affecte :

1. **Plateformes Cisco ASA**
   - Équipements matériels Cisco ASA (tous modèles)
   - Module de service ASA (ASA-SM)
   - ASA virtuel (ASAv)
   - Firmware ASA sur les plateformes Firepower 2100 / 4100 / 9300

2. **Plateformes Cisco Firepower et Secure Firewall**
   - Série Firepower 1000
   - Série Firepower 2100
   - Série Firepower 4100
   - Série Firepower 9300
   - Série Secure Firewall 200
   - Série Secure Firewall 1200
   - Série Secure Firewall 3100
   - Série Secure Firewall 4200
   - Série Secure Firewall 6100
   - Logiciel Cisco FTD (Firepower Threat Defense)

Implications

1. **CVE-2025-20362 – Contournement de l'authentification :** L'attaquant envoie des requêtes HTTP/HTTPS non authentifiées vers des points de terminaison d'URL restreints sur le serveur web VPN de l'appareil. L'absence de vérification d'autorisation permet à ces requêtes de réussir sans aucune identification valide.

2. **CVE-2025-20333 – Exécution de code à distance :** Une fois l'accès aux points de terminaison restreints établi, l'attaquant envoie des requêtes HTTPS spécialement conçues qui déclenchent un dépassement de mémoire tampon classique dans le composant serveur web VPN. Cela entraîne l'exécution de code arbitraire sur l'appareil, généralement avec des privilèges de niveau root.

3. **Injection dans le processus LINA :** FIRESTARTER lit la mémoire du processus LINA (le moteur principal de traitement réseau de l'appareil) et vérifie des motifs spécifiques en mémoire afin de confirmer que la cible est adaptée.

4. **Remplacement du gestionnaire :** FIRESTARTER écrase en mémoire le pointeur de fonction d'un gestionnaire XML WebVPN légitime et le remplace par un pointeur vers son propre shellcode malveillant de deuxième étape. Toutes les requêtes WebVPN entrantes sont désormais interceptées par l'attaquant.

5. **Déclencheur par octet magique :** Le gestionnaire malveillant inspecte les données des requêtes XML WebVPN entrantes à la recherche d'un préfixe spécifique défini sur mesure (octets magiques). Lorsque le motif est détecté, le shellcode qui le suit immédiatement est exécuté en mémoire, permettant à l'attaquant d'exécuter n'importe quelle commande.

6. **Persistance au démarrage via CSP_MOUNT_LIST :** FIRESTARTER manipule la liste de montage de la Cisco Service Platform (CSP_MOUNT_LIST) afin d'être ré-exécuté lors de la séquence de démarrage de l'appareil. Lorsqu'un redémarrage normal ou un signal de terminaison survient, FIRESTARTER se copie vers un emplacement de sauvegarde (/opt/cisco/platform/logs/var/log/svc_samcore.log) et met à jour la liste de montage pour se restaurer au prochain démarrage.

7. **Nettoyage forensique :** Après chaque exécution, FIRESTARTER restaure la CSP_MOUNT_LIST originale à partir d'une copie temporaire, s'efface du disque et supprime toutes ses traces, donnant l'illusion que l'appareil est propre lors d'une inspection.

Mesures d'atténuation

CERTVU recommande les mesures suivantes :

Appliquer tous les correctifs nécessaires

- **Appliquer les mises à jour logicielles afin de remédier aux vulnérabilités CVE-2025-20333 et CVE-2025-20362**, si cela n'a pas déjà été effectué.
- Appliquer le correctif récemment publié par Cisco, spécifiquement conçu pour neutraliser le mécanisme de persistance FIRESTARTER (se référer aux instructions CISA relatives aux Core Dumps et à la détection pour les liens propres à chaque équipement).
- Appliquer toutes les mises à jour ultérieures via le portail de téléchargement de Cisco dans un délai de 48 heures suivant leur publication.

Références

1. https://www.cisa.gov/news-events/directives/v1-ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices
2. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-persist-CISAED25-03

.