ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

BULLETIN DE SECURITE

Titre	Zero-day critiques dans Cisco ASA et FTD
Numéro de Référence	57072609/25
Date de Publication	26 Septembre 2025
Risque	Critique
Impact	Critique

Systèmes affectés

- Adaptive Security Appliance (ASA) versions 9.12.x antérieures à 9.12.4.72
- Adaptive Security Appliance (ASA) versions 9.14.x antérieures à 9.14.4.28
- Adaptive Security Appliance (ASA) versions 9.16.x antérieures à 9.16.4.85
- Adaptive Security Appliance (ASA) versions 9.17.x et 9.18.x antérieures à 9.18.4.67
- Adaptive Security Appliance (ASA) versions 9.19.x et 9.20.x antérieures à 9.20.4.10
- Adaptive Security Appliance (ASA) versions 9.22.x antérieures à 9.22.2.14
- Adaptive Security Appliance (ASA) versions 9.23.x antérieures à 9.23.1.19
- Firewall Threat Defense (FTD) versions 7.0.x antérieures à 7.0.8.1
- Firewall Threat Defense (FTD) versions 7.1.x et 7.2.x antérieures à 7.2.10.2
- Firewall Threat Defense (FTD) versions 7.3.x et 7.4.x antérieures à 7.4.2.4
- Firewall Threat Defense (FTD) versions 7.6.x antérieures à 7.6.2.1
- Firewall Threat Defense (FTD) versions 7.7.x antérieures à 7.7.10.1

NB : Les équipements Cisco Secure Firewall Adaptive Security Appliance (ASA) Software et Cisco Secure Firewall Threat Defense (FTD) Software exécutant des versions vulnérables avec l'une des configurations suivantes :

- AnyConnect IKEv2 Remote Access (crypto ikev2 enable ... client-services)
- Mobile User Security (MUS) (webvpn mus ...)
- SSL VPN (webvpn enable ...)

Identificateurs externes

- CVE-2025-20333, CVE-2025-20362

Bilan de la vulnérabilité

Cisco a publié un avertissement concernant deux vulnérabilités critiques de type zero-day dans le VPN Web Server de Cisco Secure Firewall Adaptive Security Appliance (ASA) Software et Cisco Secure Firewall Threat Defense (FTD) Software. Ces failles peuvent permettre à des attaquants d'accéder à des ressources restreintes ou d'exécuter du code arbitraire avec des privilèges « root ».

Les détails des deux vulnérabilités sont les suivants :

- CVE-2025-20333 (CVSS 9.9 – Critique) : Une faille de validation des entrées HTTP(S) permettant à un attaquant authentifié avec des identifiants VPN valides d'exécuter du code arbitraire en tant que « root » sur l'équipement ciblé. Une exploitation réussie peut entraîner la compromission totale du pare-feu.

- CVE-2025-20362 (CVSS 6.5 – Important) : Une autre faille de validation des entrées HTTP(S) pouvant permettre à un attaquant non authentifié d'accéder à des URL restreintes sans fournir d'identifiants, augmentant le risque d'accès non autorisé et facilitant des attaques combinées.

Cisco a confirmé que ces vulnérabilités sont activement exploitées et recommande vivement d'appliquer immédiatement les mises à jour correctives publiées.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 25 Septembre 2025, afin d'installer les dernières mises à jour de sécurité.

Risque

- Exécution du code arbitraire à distance
- Accès aux informations confidentielles
- Elévation de privilèges

Annexe

Bulletin de sécurité Cisco du 25 Septembre 2025**:**

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-YROOTUW
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-z5xP8EUB

Guide de détection Cisco du 25 septembre 2025 :

- https://sec.cloudapps.cisco.com/security/center/resources/detection_guide_for_continued_attacks