AVIS DE SECURITE

Objet	Multiples vulnérabilités critiques dans Cisco Secure Firewall ASA, FTD et FMC, durcissement logiciel (deux vulnérabilités activement exploitées)
Niveau de criticité	**CRITIQUE**
Référence	SNCSIRT-2026-ADS-207
TLP	WHITE

Résumé

L'équipe d'ingénierie de Cisco Secure Firewall Adaptive Security Appliance (ASA), Secure Firewall Threat Defense (FTD) et Secure Firewall Management Center (FMC) a publié le 16 septembre 2026, à l'issue d'une revue de sécurité interne, une release de durcissement logiciel corrigeant 18 vulnérabilités, dont plusieurs critiques permettant une exécution de code arbitraire à distance avec les privilèges root. Cisco indique que deux de ces vulnérabilités sont activement exploitées. Parmi les failles les plus sévères figurent un traitement incorrect d'un flux d'octets Java non authentifié et une vulnérabilité du tunnel sftunnel permettant un accès root non authentifié.

Risque de sécurité

- Exécution de code arbitraire à distance avec privilèges root (CVE-2026-20324, CVE-2026-20329, CVSS 9.9)
- Contournement du contrôle d'accès (CVE-2026-20330, CVE-2026-20332, CVSS 9.9)
- Traitement incorrect de conditions exceptionnelles (CVE-2026-20331, CVSS 9.6)
- Élévation de privilèges (CVE-2026-20333, CVE-2026-20336, CVSS 8.8)
- Atteinte à la confidentialité des données (CVE-2026-20334, CVSS 8.4)

Systèmes affectés

- Cisco Secure Firewall Adaptive Security Appliance (ASA) Software — versions antérieures aux correctifs du 16 septembre 2026
- Cisco Secure Firewall Threat Defense (FTD) Software — versions antérieures aux correctifs du 16 septembre 2026
- Cisco Secure Firewall Management Center (FMC) Software — versions antérieures aux correctifs du 16 septembre 2026

Recommandations

Se référer au bulletin de sécurité de l'éditeur du 16 septembre 2026 :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-asaftdfmc-uvpPROhN
- https://securityonline.info/cisco-secure-firewall-vulnerabilities-september-2026/