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	Vulnérabilités critiques dans les produits Cisco
Numéro de Référence	61680503/26
Date de Publication	05 Mars 2026
Risque	Critique
Impact	Critique

Systèmes affectés

- Adaptive Security Appliance ;
- Cisco 3000 Series Industrial Security Appliances (ISA);
- Cisco ASA 5500-X Series Firewalls ;
- Cisco Adaptive Security Virtual Appliance (ASAv);
- Cisco Firepower 1000 Series ;
- Cisco Firepower 2100 Series ;
- Cisco Firepower 9000 Series ;
- Cisco Secure Endpoint ;
- Cisco Secure Firewall 3100 Series ;
- Cisco Secure Firewall 4200 Series ;
- Cisco Secure Firewall Adaptive Security Appliance (ASA) Software;
- Cisco Secure Firewall Management Center ;
- Cisco Secure Firewall Management Center (FMC);
- Cisco Secure Firewall Management Center (FMC) Appliances;
- Cisco Secure Firewall Threat Defense (FTD) Software;
- Firepower Management Center ;
- Firepower Threat Defense ;

Identificateurs externes

- CVE-2024-20340 CVE-2024-20358 CVE-2026-20001 CVE-2026-20002 CVE-2026-20003
- CVE-2026-20006 CVE-2026-20007 CVE-2026-20008 CVE-2026-20009 CVE-2026-20013
- CVE-2026-20014 CVE-2026-20015 CVE-2026-20016 CVE-2026-20017 CVE-2026-20018

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

- CVE-2026-20020 CVE-2026-20021 CVE-2026-20022 CVE-2026-20023 CVE-2026-20024
- CVE-2026-20025 CVE-2026-20031 CVE-2026-20039 CVE-2026-20044 CVE-2026-20049
- CVE-2026-20050 CVE-2026-20052 CVE-2026-20062 CVE-2026-20063 CVE-2026-20064
- CVE-2026-20069 CVE-2026-20070 CVE-2026-20073 CVE-2026-20082 CVE-2026-20100
- CVE-2026-20101 CVE-2026-20102 CVE-2026-20103 CVE-2026-20105 CVE-2026-20106

Bilan de la vulnérabilité

Plusieurs vulnérabilités critiques ont été corrigées dans les versions susmentionnées des produits Cisco. Un attaquant distant pourrait exploiter certaines de ces vulnérabilités pour provoquer un déni de service, une élévation de privilège, une usurpation d'identité, une exécution de code à distance, une divulgation d'informations sensibles et un contournement de la politique de sécurité sur le système affecté.

Solution

Veuillez se référer au bulletin de sécurité Cisco du 04 Mars 2026 pour plus d'information.

Risque

- Déni de service ;
- Elévation de privilèges ;
- Contournement de la politique de sécurité ;
- Exécution du code arbitraire à distance ;
- Usurpation d'identité ;

Annexe

Bulletin de sécurité Cisco du 04 Mars 2026:

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-dos-FCvLD6vR
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-scpcxt-filecpy-rgeP73nE
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ssh keybypass-cr5xPUSf
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-aclbypass-dos-CVxVRSvQ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmd-inj-ZJV8Wysm
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-desync-n5AVzEQw
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-esp-dos-uv7yD8P5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-eBueGdEG

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-luainject-VescqgmS
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ospf-ZH8PhbSW
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-saml-LktTrwZP
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-SpOFF2Re
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-m9sx6MbC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-webvpn-xss-uwjc4HR
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-css-Fn4QSZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inject-S9ZM4EJf
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sql-inject-2EnmTC8v
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-sql-injection-2qH6CcJd
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmd-inj-mTzGZexf
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dd-dos-bpEcg7B7
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort-bypass-rLggKzVF
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort3ssl-FBEKYXpH
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tcp-dos-rHfqnwRg
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftdfmc-dir-trav-wERgjhWq
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5JPp45V2