



.....
Centre de Veille de Détection et de
Réaction aux Attaques Informatiques

BULLETIN DE SECURITE

Titre	Vulnérabilités affectant des produits de Cisco
Numéro de Référence	56291508/25
Date de publication	15 Aout 2025
Risque	Critique
Impact	Critique

Systemes affectés

- Cisco Secure Firewall Management Center Software
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software
- Cisco IOS, IOS XE, Secure Firewall Adaptive Security Appliance, and Secure Firewall Threat Defense Software
- Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense Software for Firepower 2100 Series
- Cisco Secure Firewall Threat Defense Software
- Cisco Secure Firewall Management Center Software

Identificateurs externes

CVE-2025-20127	CVE-2025-20133	CVE-2025-20134	CVE-2025-20135	CVE-2025-20136
CVE-2025-20148	CVE-2025-20217	CVE-2025-20218	CVE-2025-20219	CVE-2025-20220
CVE-2025-20222	CVE-2025-20224	CVE-2025-20225	CVE-2025-20235	CVE-2025-20237
CVE-2025-20238	CVE-2025-20239	CVE-2025-20243	CVE-2025-20244	CVE-2025-20251
CVE-2025-20252	CVE-2025-20253	CVE-2025-20254	CVE-2025-20263	CVE-2025-20265
CVE-2025-20268	CVE-2025-20301	CVE-2025-20302	CVE-2025-20306	

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités affectant certaines versions de ses produits susmentionnés. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code, d'injecter des commandes ou de causer un déni de service.

Solution

Veuillez se référer aux bulletins de sécurité de Cisco pour mettre à jours vos produits.

Risques

- Exécution de code
- Injection de commandes
- Déni de service

Références

Bulletins de sécurité de Cisco :

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3100_4200_tlstdos-2yNSCd54
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-buffer-overflow-PyRUhWBC>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-acl-bypass-mtPze9Yh>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ios-dos-DOESHWy>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-cmdinj-VEhFeZQ3>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dhcp-qj7nGs4N>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-http-file-hUyX2jL4>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-nat-dns-dos-bqhynHTM>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa->

asaftd-sslts-dos-eHw76vZe

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpn-dos-mfPekA6e>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-vpnwebs-dos-hjBhmBsX>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-authz-bypass-M7xhnAu>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-cmd-inj-HCRLpFyN>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-ftd-cmdinj-PhE7kmT>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-html-inj-MqjrZrny>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-radius-rce-TNBKf79>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xpathinj-COrThdMb>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-JtNmcusP>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fp2k-IPsec-dos-tjwgDZCO>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-SvKhtjgt>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-ravpn-geobypass-9h38M37Z>