DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 28-03-2026

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Cisco
Réference	1451
Date de Publication	2026-03-27
Sévérité	Elevé

IMPACT :

- Exécution de code à distance
- Contournement de mesures de sécurité
- Accès à des informations confidentielles
- Elévation de privilèges
- Déni de service

SYSTÉME AFFECTÉ :

- Cisco Catalyst SD-WAN Manager
- Cisco IOS Software
- Cisco IOS XE Software
- Cisco IOS XE Wireless Controller Software
- Cisco Secure Firewall Adaptive Security Appliance Software
- Cisco Secure Firewall Threat Defense Software

DÉSCRIPTION :

Cisco a identifié et corrigé plusieurs vulnérabilités affectant certaines versions de ses produits mentionnés. L'exploitation de ces failles pourrait permettre à un attaquant d'exécuter du code à distance, de contourner des mécanismes de sécurité, d'accéder à des informations sensibles, d'escalader ses privilèges ou de provoquer un déni de service.

SOLUTION :

Mettre à jour les produits Cisco(se référer à la documentation).

DOCUMENTATION :

- Bulletins de sécurité de Cisco :

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ios-dos-kPEpQGGK

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bootp-WuBhNBxA

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ios-http-dos-sbv8XRpL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-lobby-privesc-KwxBqJy

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-mntc-dos-LZweQcyq

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-tls-dos-TVgLDEZL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe_infodis-6J847uEB

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-crlf-NvgKTKJZ

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iox-xss-LpGkzwtJ

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-scp-dos-duAdXtCg

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmanage-xss-ZqkhP9W9

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-dos-hnX5KGOm

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xe-secureboot-bypass-B6uYxYSZ

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh

- CVE-2026-20004:

https://nvd.nist.gov/vuln/detail/CVE-2026-20004

- CVE-2026-20012:

https://www.tenable.com/cve/CVE-2026-20012

- CVE-2026-20083:

https://nvd.nist.gov/vuln/detail/CVE-2026-20083

- CVE-2026-20084:

https://www.tenable.com/cve/CVE-2026-20084

- CVE-2026-20086:

https://www.tenable.com/cve/CVE-2026-20086

- CVE-2026-20104:

https://nvd.nist.gov/vuln/detail/CVE-2026-20104

- CVE-2026-20108:

https://nvd.nist.gov/vuln/detail/CVE-2026-20108

- CVE-2026-20110:

https://nvd.nist.gov/vuln/detail/CVE-2026-20110

- CVE-2026-20112:

https://nvd.nist.gov/vuln/detail/CVE-2026-20112

- CVE-2026-20113:

https://nvd.nist.gov/vuln/detail/CVE-2026-20113

- CVE-2026-20114:

https://nvd.nist.gov/vuln/detail/cve-2026-2014

- CVE-2026-20115:

https://nvd.nist.gov/vuln/detail/CVE-2026-2015

- CVE-2026-20125:

https://nvd.nist.gov/vuln/detail/CVE-2026-20125

- CVE-2026-20131:

https://nvd.nist.gov/vuln/detail/CVE-2026-20131