Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0104

Kwetsbaarheden verholpen in Cisco IOS XE Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 26-03-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Cisco heeft kwetsbaarheden verholpen in Cisco IOS XE Software, specifiek voor verschillende producten zoals Catalyst 9000 Series Switches, Catalyst CW9800 Family, en Cisco Meraki.

Duiding

De kwetsbaarheden omvatten verschillende problemen, zoals een geheugenlek in de IKEv2-implementatie, kwetsbaarheden in de DHCP-snooping functie, en onjuiste verwerking van CAPWAP-pakketten die leiden tot een denial of service. Daarnaast zijn er kwetsbaarheden gerapporteerd die het mogelijk maken voor ongeauthenticeerde aanvallers om toegang te krijgen tot gevoelige apparaatconfiguraties en om privileges te verhogen via de Lobby Ambassador API. Ook zijn er problemen met onjuiste privilege-toewijzingen en een kritieke kwetsbaarheid in de bootloader die lokale of fysieke toegang vereisen voor exploitatie. De SCP-serverfunctie is ook kwetsbaar voor denial of service door onjuiste verwerking van SCP-verzoeken.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- 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-dhcpsn-dos-xBn8Mtks#fs
- 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-scp-dos-duAdXtCg
- 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

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20012	8.6 HIGH
CVE-2026-20084	8.6 HIGH
CVE-2026-20086	8.6 HIGH
CVE-2026-20004	7.4 HIGH
CVE-2026-20115	6.1 MEDIUM
CVE-2026-20125	7.7 HIGH
CVE-2026-20114	5.4 MEDIUM
CVE-2026-20110	6.5 MEDIUM
CVE-2026-20104	6.1 MEDIUM
CVE-2026-20083	6.5 MEDIUM

CWE's

CWE	Beschrijving
CWE-124	Buffer Underwrite ('Buffer Underflow')
CWE-228	Improper Handling of Syntactically Invalid Structure
CWE-230	Improper Handling of Missing Values
CWE-235	Improper Handling of Extra Parameters
CWE-266	Incorrect Privilege Assignment
CWE-319	Cleartext Transmission of Sensitive Information
CWE-400	Uncontrolled Resource Consumption
CWE-401	Missing Release of Memory after Effective Lifetime

CWE-771	Missing Reference to Active Allocated Resource
CWE-1286	Improper Validation of Syntactic Correctness of Input

Getroffen producten

Cisco
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 IOS XE Software
Cisco Secure Firewall 3100 Series
Cisco Secure Firewall 4200 Series
Cisco Secure Firewall Adaptive Security Appliance (ASA) Software
Cisco Secure Firewall Threat Defense (FTD) Software
IOS

Disclaimer