Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0146

## Kwetsbaarheden verholpen in Cisco IOS XE Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 08-05-2025

**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.

## Duiding

De kwetsbaarheden in Cisco IOS XE Software omvatten verschillende problemen, waaronder onvoldoende invoervalidatie en onjuist geheugenbeheer. Deze kwetsbaarheden kunnen worden misbruikt door ongeauthenticeerde aanvallers om Denial-of-Service (DoS) situaties te veroorzaken, ongeautoriseerde toegang te verkrijgen, en zelfs om configuraties te manipuleren. Kwetsbare systemen kunnen onverwacht opnieuw opstarten of kunnen worden blootgesteld aan ongeautoriseerde commando-injectie-aanvallen, wat de integriteit en beschikbaarheid van netwerken in gevaar kan brengen.

## 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-ewlc-cdp-dos-fpeks9K
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-multi-ARNHM4v6
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-ikev1-dos-XHk3HzFC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ewlc-user-del-hQxMpUDj
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr903-rsp3-arp-dos-WmfzdvJZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-file-uplpd-rHZG9UfC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-webui-cmdinj-gVn3OKNC
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-dhcpsn-dos-xBn8Mtks
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-twamp-kV4FHugn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wlc-wncd-p6Gvt6HL

## Kwetsbaarheden

| CVE | CVSS Score |
|---|---|
| CVE-2025-20137 | 4.7 MEDIUM |
| CVE-2025-20140 | 7.4 HIGH |
| CVE-2025-20154 | 8.6 HIGH |
| CVE-2025-20162 | 8.6 HIGH |
| CVE-2025-20181 | 6.8 MEDIUM |
| CVE-2025-20182 | 8.6 HIGH |
| CVE-2025-20186 | 8.8 HIGH |
| CVE-2025-20188 | 10.0 CRITICAL |
| CVE-2025-20189 | 7.4 HIGH |
| CVE-2025-20190 | 6.5 MEDIUM |
| CVE-2025-20192 | 7.7 HIGH |
| CVE-2025-20194 | 5.4 MEDIUM |
| CVE-2025-20202 | 7.4 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-762 | Mismatched Memory Management Routines |
| CWE-805 | Buffer Access with Incorrect Length Value |
| CWE-347 | Improper Verification of Cryptographic Signature |
| CWE-232 | Improper Handling of Undefined Values |
| CWE-798 | Use of Hard-coded Credentials |
| CWE-352 | Cross-Site Request Forgery (CSRF) |

| | |
|---|---|
| CWE-284 | Improper Access Control |
| CWE-400 | Uncontrolled Resource Consumption |
| CWE-78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |
| CWE-787 | Out-of-bounds Write |
| CWE-789 | Memory Allocation with Excessive Size Value |
| CWE-20 | Improper Input Validation |

## Getroffen producten

| **Cisco** |
|---|
| Cisco IOS XE Software |

## Disclaimer