Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0043

## Kwetsbaarheden verholpen in Cisco IOS, IOS XE en IOS XR Software

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-02-2025
Revisie: 1.0.1

**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

## Update Revisie 1

Door een technisch issue is deze advisory eerder verstuurd met een invalide signature, waardoor automatische verwerking mogelijk verstoord is. Deze update verhelpt dat. Er is verder geen inhoudelijke wijziging.

## Feiten

Cisco heeft meerdere kwetsbaarheden verholpen in IOS, IOS XE en IOS XR Software.

## Duiding

De kwetsbaarheden bevinden zich in de wijze waarop het SNMP-subsystem op de kwetsbare apparaten verkeer verwerkt. Geauthenticeerde kwaadwillenden kunnen speciaal vervaardigde SNMP-verzoeken verzenden, wat kan leiden tot Denial-of-Service (DoS) condities op de getroffen apparaten. De impact kan variëren afhankelijk van de specifieke softwareversie die in gebruik is. Deze kwetsbaarheden vormen een aanzienlijk risico voor de netwerkbeschikbaarheid en kunnen een breed scala aan Cisco-apparaten beïnvloeden.

## 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-snmp-dos-sdxnSUcW
- https://sec.cloudapps.cisco.com/security/center/publicationService.x?limit=20

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2025-20169 | 7.7 HIGH |
| CVE-2025-20170 | 7.7 HIGH |
| CVE-2025-20171 | 7.7 HIGH |
| CVE-2025-20172 | 7.7 HIGH |

| | |
|---|---|
| CVE-2025-20173 | 7.7 HIGH |
| CVE-2025-20174 | 7.7 HIGH |
| CVE-2025-20175 | 7.7 HIGH |
| CVE-2025-20176 | 7.7 HIGH |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-805 | Buffer Access with Incorrect Length Value |

## Getroffen producten

| **cisco** |
|---|
| cisco_ios_xe_software |
| cisco_ios_xr_software |
| ios |

## Disclaimer