



## Advisory NCSC-2026-0411

PRIORITEIT: NORMAAL

# Kwetsbaarheden verholpen in Cisco networking producten

Publicatiedatum: 09-10-2026

Toegestane verspreiding: TLP:WHITE  
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl).

## Feiten

Cisco heeft meerdere kwetsbaarheden verholpen in Cisco IOS XE Software.

## Duiding

De kwetsbaarheden zijn intern door Cisco's engineering teams ontdekt tijdens beveiligingsreviews. Deze kwetsbaarheden zijn van invloed op Cisco IOS XE-software wanneer deze in autonome modus of controllermodus wordt uitgevoerd, ongeacht de apparaatconfiguratie. De geïdentificeerde problemen betreffen onder andere onjuiste access control, buffer management fouten, onjuiste resource control en onjuiste input validatie.

## Oplossingen

Cisco heeft software hardening 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-hardening-iosxe-V8NMuMZJ>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-meraki-os-drbEX9GH>

## Kwetsbaarheden

| CVE            | CVSS Score   |
|----------------|--------------|
| CVE-2026-76463 | 8.8 HIGH     |
| CVE-2026-76464 | 9.6 CRITICAL |
| CVE-2026-76467 | 7.5 HIGH     |
| CVE-2026-76468 | 8.2 HIGH     |
| CVE-2026-76469 | 7.4 HIGH     |

| CVE            | CVSS Score |
|----------------|------------|
| CVE-2026-76470 | 8.8 HIGH   |
| CVE-2026-76472 | 8.8 HIGH   |

## CWE's

| CWE     | Beschrijving                   |
|---------|--------------------------------|
| CWE-125 | Out-of-bounds Read             |
| CWE-190 | Integer Overflow or Wraparound |

## Getroffen producten

|                                                 |
|-------------------------------------------------|
| Cisco                                           |
| Cisco Campus Gateway Software                   |
| Cisco Meraki MR Wireless Access Points Software |
| Meraki MR                                       |
| Meraki MS                                       |
| Meraki MX                                       |
| iOS XE                                          |

## Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:

NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy or incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.