



# NCSC-2026-0036

## Kwetsbaarheden verholpen in Cisco Unified Communications producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 22-01-2026

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

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

## Feiten

Cisco heeft kwetsbaarheden verholpen in verschillende Cisco Unified Communications producten.

## Duiding

De kwetsbaarheden omvatten een kritieke kwetsbaarheid die ongeauthenticeerde externe aanvallers in staat stelt om willekeurige commando's op het besturingssysteem van het apparaat uit te voeren. Dit is te wijten aan onjuiste validatie van gebruikersinvoer in HTTP-verzoeken, wat aanvallers in staat kan stellen om gebruikersniveau toegang te krijgen en mogelijk hun privileges naar root te verhogen. Daarnaast zijn er meerdere kwetsbaarheden in de webgebaseerde beheersinterfaces van Cisco Packaged Contact Center Enterprise en Cisco Unified Contact Center Enterprise, die kunnen worden misbruikt door geauthenticeerde externe aanvallers voor cross-site scripting (XSS) aanvallen. Ook bevat de Cisco Intersight Virtual Appliance een kwetsbaarheid in de read-only onderhoudshell die geauthenticeerde lokale aanvallers met administratieve privileges in staat stelt om hun privileges naar root te verhogen. Tot slot is er een kwetsbaarheid in de SSH-service van Cisco IEC6400 Wireless Backhaul Edge Compute Software die ongeauthenticeerde externe aanvallers in staat stelt om een denial of service (DoS) aanval te initiëren, waardoor de SSH-service onresponsief wordt.

## 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-iec6400-Pem5uQ7v>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-intersight-privesc-p6tBm6jk>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucce-pcce-xss-2JVyg3uD>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-voice-rce-mORhqY4b>

## Kwetsbaarheden

| CVE              | CVSS Score |
|------------------|------------|
| ➤ CVE-2026-20045 | 8.2 HIGH   |
|                  |            |

|                  |            |
|------------------|------------|
| ➤ CVE-2026-20055 | 4.8 MEDIUM |
| ➤ CVE-2026-20092 | 6.0 MEDIUM |
| ➤ CVE-2026-20109 | 4.8 MEDIUM |
| ➤ CVE-2026-20080 | 5.3 MEDIUM |

CWE's

| CWE       | Beschrijving                                                                         |
|-----------|--------------------------------------------------------------------------------------|
| ➤ CWE-79  | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |
| ➤ CWE-94  | Improper Control of Generation of Code ('Code Injection')                            |
| ➤ CWE-400 | Uncontrolled Resource Consumption                                                    |
| ➤ CWE-732 | Incorrect Permission Assignment for Critical Resource                                |

Getroffen producten

|                                                           |
|-----------------------------------------------------------|
| Cisco                                                     |
| Cisco Intersight Virtual Appliance                        |
| Cisco Packaged Contact Center Enterprise                  |
| Cisco Ultra-Reliable Wireless Backhaul                    |
| Unified Communications Manager                            |
| Unified Communications Manager IM and Presence Service    |
| Unified Communications Manager Session Management Edition |
|                                                           |

Unity  
Connection

## 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 of 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.