



# NCSC-2025-0204

## Kwetsbaarheden verholpen in Cisco ISE en ISE-PIC

NCSC Advisory

**PRIORITEIT: HOOG**

Gepubliceerd op: 26-06-2025

**TLP:WHITE**

### Toegepaste 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 Cisco ISE en ISE-PIC.

## Duiding

De kwetsbaarheden bevinden zich in de manier waarop Cisco ISE en ISE-PIC bestanden verwerken via APIs en gebruikersinvoer valideren. Ongeauthenticeerde aanvallers met toegang tot de API-interface kunnen deze kwetsbaarheden misbruiken om willekeurige bestanden te uploaden en uit te voeren met root-rechten, evenals om commando's op het onderliggende besturingssysteem uit te voeren. Dit kan leiden tot volledige compromittatie van het kwetsbare systeem.

Het is belangrijk om te vermelden dat de twee kwetsbaarheden in kwestie zijn geïntroduceerd in de recentere versies 3.3 en 3.4. Cisco geeft aan dan versies 3.2 en daarvoor niet kwetsbaar zijn en dat de kwetsbaarheid met kenmerk CVE-2025-20282 niet van toepassing is op versie 3.3

## 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-ise-unauth-rce-ZAd2GnJ6>

## Kwetsbaarheden

CVE	CVSS Score
➤ <a href="#">CVE-2025-20282</a>	10.0 CRITICAL
➤ <a href="#">CVE-2025-20281</a>	9.8 CRITICAL

## CWE's

CWE	Beschrijving
➤ <a href="#">CWE-74</a>	

Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')

➤ [CWE-269](#)

Improper Privilege Management

## Getroffen producten

### Cisco

Cisco Identity Services Engine  
Software

## 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.