Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2024-0432

## Kwetsbaarheden verholpen in Cisco Identity Services Engine

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 07-11-2024

**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 Identity Services Engine (ISE)

## Duiding

De kwetsbaarheden bevinden zich in de management-interface en stellen een kwaadwillende in staat om een Cross-Site-Scripting-aanval uit te voeren. Een dergelijke aanval kan leiden tot uitvoer van willekeurige code in de browser van het slachtoffer, of toegang tot gevoelige gegevens in de context van de browser van het slachtoffer.

Omdat de kwetsbaarheden zich in de management-interface bevinden, is niet uit te sluiten dat het slachtoffer met verhoogde rechten werkt, waardoor uitvoer van code met verhoogde rechten kan plaatsvinden.

Succesvol misbruik vereist wel dat de kwaadwillende toegang heeft tot de management-interface. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheer-omgeving.

## 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-auth-bypass-BBRf7mkE
› https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-vuln-DBQdWRy

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| › CVE-2024-20525 | **6.1 MEDIUM** |
| › CVE-2024-20527 | **5.5 MEDIUM** |
| › CVE-2024-20529 | **5.5 MEDIUM** |
| › CVE-2024-20530 | **6.1 MEDIUM** |

| | |
|---|---|
| CVE-2024-20531 | **5.5 MEDIUM** |
| CVE-2024-20532 | **5.5 MEDIUM** |
| CVE-2024-20537 | **6.5 MEDIUM** |
| CVE-2024-20538 | **6.1 MEDIUM** |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-863 | Incorrect Authorization |
| CWE-22 | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| CWE-611 | Improper Restriction of XML External Entity Reference |
| CWE-79 | Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

## Getroffen producten

| **cisco** |
|---|
| cisco_identity_services_engine_software |
| identity_services_engine |

## Disclaimer