



NCSC-2025-0365

Kwetsbaarheden verholpen in Cisco Catalyst Center

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 14-11-2025

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 Cisco Catalyst Center.

Duiding

Deze kwetsbaarheid met kenmerk CVE-2025-20341, ontstaat door onvoldoende validatie van gebruikersinvoer. Een kwaadwillende kan dit misbruiken, door een speciaal vervaardigd HTTP-verzoek te versturen, waardoor ongeautoriseerde systeemwijzigingen mogelijk worden, zoals het aanmaken van accounts of het verhogen van eigen rechten.

De kwetsbaarheid met kenmerk CVE-2025-20353, kan een niet-geauthenticeerde, externe aanvaller in staat stellen om een cross-site scripting (XSS)-aanval uit te voeren. Deze kwetsbaarheid wordt veroorzaakt door onvoldoende validatie van gebruikersinvoer. Door een gebruiker te laten klikken op een speciaal gemaakte link, kan de aanvaller willekeurige code uitvoeren of toegang krijgen tot gevoelige browserinformatie.

De kwetsbaarheid met kenmerk CVE-2025-20346 kan een geauthenticeerde, externe aanvaller in staat stellen om handelingen uit te voeren die normaal Administrator-rechten vereisen. De aanvaller heeft hiervoor geldige read-only gebruikersgegevens nodig. Deze kwetsbaarheid ontstaat door onjuiste rolgebaseerde toegangscontrole (RBAC). Een aanvaller kan hiervan misbruik maken door in te loggen op een getroffen systeem en bepaalde beleidsconfiguraties aan te passen.

De kwetsbaarheid met kenmerk CVE-2025-20349, in de REST API van Cisco Catalyst Center maakt het een geauthenticeerde aanvaller mogelijk om willekeurige opdrachten als root uit te voeren in een beperkte container door een speciaal vervaardigd API-verzoek te versturen.

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-catc-priv-esc-VS8EeCuX>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-ci-ZWLQVSwT>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnac-xss-weXtVZ59>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-privesc-catc-rYjReeLU>

Kwetsbaarheden

CVE	CVSS Score
> CVE-2025-20353	6.1 MEDIUM
> CVE-2025-20349	6.3 MEDIUM
> CVE-2025-20346	4.3 MEDIUM
> CVE-2025-20341	8.8 HIGH

CWE's

CWE	Beschrijving
> CWE-284	Improper Access Control
> CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-269	Improper Privilege Management

Getroffen producten

Cisco
Catalyst

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.