



NCSC-2025-0183

Kwetsbaarheid verholpen in Cisco Identity Services Engine voor cloudplatformen

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 05-06-2025

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 een kwetsbaarheid verholpen in Identity Services Engine (ISE) voor cloudplatformen.

Duiding

De kwetsbaarheid betreft een fout bij het automatisch genereren van wachtwoorden wanneer Cisco ISE op een cloudplatform wordt geïnstalleerd. Hierdoor worden in verschillende ISE-cloudomgevingen dezelfde wachtwoorden gebruikt. Een ongeauthenticeerde kwaadwillende op afstand kan hierdoor toegang krijgen tot gevoelige gegevens, beperkte beheerrechten op de ISE-omgeving bemachtigen en configuratiewijzigingen doorvoeren.

De kwetsbaarheid treft ISE voor Amazon Web Services (AWS), Microsoft Azure en Oracle Cloud Infrastructure (OCI). De kwetsbaarheid doet zich alleen voor wanneer de Primary Administration-node in de cloudomgeving is geïnstalleerd. Omgevingen waar de Primary Administration-node on-premise draait, zijn niet kwetsbaar. Daarnaast zijn enkele specifieke cloudimplementaties niet kwetsbaar. Zie de bijgevoegde referentie voor meer informatie.

Oplossingen

Cisco heeft hotfixes uitgebracht waarmee de kwetsbaarheid wordt verholpen. Zie de bijgevoegde referentie voor meer informatie.

Referenties

➤ <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-aws-static-cred-FPMjUcm7>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-20286	9.9 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-259	Use of Hard-coded Password

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.