Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0208

Kwetsbaarheden verholpen in Cisco Identity Services Engine

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-06-2026

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Cisco heeft meerdere kwetsbaarheden verholpen in Cisco Identity Services Engine (ISE) en Cisco ISE Passive Identity Connector (ISE-PIC).

Duiding

De kwetsbaarheden kunnen door zowel geauthenticeerde als niet-geauthenticeerde aanvallers worden misbruikt. Een geauthenticeerde aanvaller met administratieve rechten kan speciaal vervaardigde HTTP-verzoeken sturen om willekeurige commando's uit te voeren, wat kan leiden tot Denial-of-Service en privilege-escalatie, waardoor de integriteit en beschikbaarheid van de systemen in het geding komen. Daarnaast kunnen sommige kwetsbaarheden leiden tot ongeautoriseerde informatieontsluiting. Niet-geauthenticeerde aanvallers kunnen eveneens willekeurige code op afstand uitvoeren en toegang krijgen tot gevoelige informatie zoals gehashte inloggegevens. De oorzaak ligt in onjuiste autorisatiecontroles bij toegang tot bepaalde bronnen binnen de systemen.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden in Cisco Identity Services Engine en Cisco ISE Passive Identity Connector te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-G5WP8vv

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20181	9.1 CRITICAL
CVE-2026-20190	7.5 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

CWE-285	Improper Authorization

Getroffen producten

Cisco
Cisco ISE Passive Identity Connector
Cisco Identity Services Engine Software

Disclaimer