Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0382

Kwetsbaarheden verholpen in Cisco Identity Services Engine (ISE)

NCSC Security Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 17-09-2026

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

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen in Cisco ISE en ISE-PIC, waaronder mogelijkheden voor niet-geauthenticeerde en laaggeprivilegieerde kwaadwillenden om via netwerktoegang ongeautoriseerde acties uit te voeren. De kwetsbaarheden hebben CVSS-scores variërend van middel tot kritiek. Van de in totaal 21 kwetsbaarheden zijn 13 als kritiek aangemerkt. Op basis van de door Cisco gepubliceerde CVSS-scores kunnen vier kwetsbaarheden zonder authenticatie op afstand worden misbruikt. Succesvol misbruik kan onder meer leiden tot het omzeilen van authenticatie- en autorisatiecontroles, het verkrijgen en wijzigen van gevoelige configuratie- en identiteitsgegevens, het uitvoeren van willekeurige code of commando's met rootrechten, SQL-injectie, het uitlezen van bestanden en het verstoren van de beschikbaarheid van getroffen systemen. Sommige kwetsbaarheden vereisen voorafgaande administratieve toegangsrechten of een specifieke configuratie, terwijl andere volledig op afstand en zonder authenticatie kunnen worden misbruikt.

Van de 13 kwetsbaarheden die als kritiek zijn aangemerkt, hebben meerdere een CVSS-score van 9,8 of hoger. Vier kwetsbaarheden, CVE-2026-20130, CVE-2026-20192, CVE-2026-76423 en CVE-2026-76460, hebben een CVSS-score van 10,0.

De kwetsbaarheid met kenmerk CVE-2026-76423 betreft een kwetsbaarheid in de REST API waarmee een niet-geauthenticeerde kwaadwillende administratieve toegang kan verkrijgen tot Cisco ISE en ISE-PIC.

De kwetsbaarheid met kenmerk CVE-2026-76460 betreft een authenticatieomzeiling in een API van Cisco ISE en ISE-PIC waarmee een niet-geauthenticeerde kwaadwillende toegang tot het getroffen systeem kan verkrijgen. Cisco meldt dat deze kwetsbaarheid actief wordt misbruikt. Na succesvolle exploitatie kunnen kwaadwillenden volgens Cisco commando's met rootrechten uitvoeren.

De kwetsbaarheden met kenmerk CVE-2026-20130 en CVE-2026-20192 betreffen door Cisco gegroepeerde kwetsbaarheden op het gebied van respectievelijk onvoldoende neutralisatie van invoer en onjuiste toegangscontrole. Cisco heeft voor deze hardening-release meerdere onderliggende kwetsbaarheden per CWE-klasse onder één CVE-ID samengebracht. De CVSS-score vertegenwoordigt daarbij de hoogst scorende onderliggende kwetsbaarheid.

Het NCSC adviseert om de beveiligingsupdates voor de kritieke kwetsbaarheden met voorrang toe te passen.

Oplossingen

Cisco heeft updates uitgebracht voor Cisco Identity Services Engine (ISE) en Cisco ISE Passive Identity Connector (ISE-PIC) om de kwetsbaarheden te verhelpen.

Cisco heeft voor de kwetsbaarheid met kenmerk CVE-2026-76460 een IoC opgenomen in de betreffende advisory. Omdat een kwaadwillende na succesvolle exploitatie rootrechten kan verkrijgen en sporen van misbruik kan verwijderen of verbergen, adviseert Cisco ook externe netwerk- en firewalllogs te controleren. Wanneer aanwijzingen voor misbruik worden aangetroffen, adviseert Cisco om de getroffen nodes opnieuw te installeren en indien nodig de configuratie vanuit een back-up te herstellen. Zie bijgevoegde advisory voor meer informatie.

Voor de kwetsbaarheden met kenmerk CVE-2026-20130 en CVE-2026-20192 heeft Cisco daarnaast software-hardeningupdates uitgebracht. Raadpleeg de bijgevoegde advisories voor meer informatie.

Referenties

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ISE-ABP-VNSW7Tn5
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-ise-XU5EwX5T
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-cmd-inj-e2CuZCYZ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-mult-vul-ymSsTLCc
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-multi-hrP9jQSQ
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-rce-se7bYU57

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20307	9.9 CRITICAL
CVE-2026-20211	9.1 CRITICAL
CVE-2026-20176	9.1 CRITICAL
CVE-2026-76423	10.0 CRITICAL
CVE-2026-76424	7.2 HIGH
CVE-2026-76425	7.6 HIGH
CVE-2026-76426	4.9 MEDIUM
CVE-2026-76427	4.9 MEDIUM

CVE-2026-76428	4.9 MEDIUM
CVE-2026-20282	4.9 MEDIUM
CVE-2026-20283	6.5 MEDIUM
CVE-2026-20284	9.1 CRITICAL
CVE-2026-20305	9.1 CRITICAL
CVE-2026-20306	9.1 CRITICAL
CVE-2026-20130	10.0 CRITICAL
CVE-2026-20192	10.0 CRITICAL
CVE-2026-20194	9.1 CRITICAL
CVE-2026-20234	9.9 CRITICAL
CVE-2026-20237	9.1 CRITICAL
CVE-2026-20287	6.5 MEDIUM
CVE-2026-76460	10.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-23	Relative Path Traversal
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-290	Authentication Bypass by Spoofing
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-502	Deserialization of Untrusted Data

CWE-522	Insufficiently Protected Credentials
CWE-641	Improper Restriction of Names for Files and Other Resources
CWE-611	Improper Restriction of XML External Entity Reference
CWE-669	Incorrect Resource Transfer Between Spheres
CWE-943	Improper Neutralization of Special Elements in Data Query Logic

Getroffen producten

Cisco
Cisco ISE Passive Identity Connector
Cisco Identity Services Engine Software
identity_services_engine

Disclaimer