Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0106

Kwetsbaarheden verholpen in Cisco Integrated Management Controller

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 03-04-2026

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 Integrated Management Controller (IMC).

Duiding

De kwetsbaarheden bevinden zich in de webgebaseerde managementinterface van Cisco IMC. Een onbevoegde externe aanvaller kan via de functionaliteit voor het wijzigen van wachtwoorden de authenticatie omzeilen door speciaal opgemaakte HTTP-verzoeken te versturen, wat leidt tot ongeautoriseerde administratieve toegang. Daarnaast kunnen geauthenticeerde aanvallers, waaronder gebruikers met alleen leesrechten, door onvoldoende inputvalidatie command injection uitvoeren en willekeurige root-commando's of code uitvoeren, wat resulteert in privilege-escalatie en volledige controle over het systeem. Verder zijn er meerdere cross-site scripting (XSS) kwetsbaarheden, waaronder opgeslagen en gereflecteerde XSS, die geauthenticeerde gebruikers met administratieve rechten in staat stellen om kwaadaardige scripts te injecteren en uit te voeren in browsers van gebruikers die met de interface werken. Ook kunnen onbevoegde externe aanvallers via gereflecteerde XSS kwetsbaarheden kwaadaardige scripts injecteren door gebruikers te verleiden op speciaal opgemaakte links te klikken, wat kan leiden tot sessiekaping en ongeautoriseerde acties binnen de context van de getroffen gebruikers. Alle kwetsbaarheden zijn het gevolg van onvoldoende inputvalidatie in de webinterface van Cisco IMC.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de management-interface. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separate beheeromgeving.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden in Cisco Integrated Management Controller te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-auth-bypass-AgG2BxTn
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-cmd-inj-3hKN3bVt
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cimc-xss-A2tkgVAB
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ucs-ssh-priv-esc-2mZDtdjM#fs

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20093	9.8 CRITICAL
CVE-2026-20094	8.8 HIGH
CVE-2026-20095	6.5 MEDIUM
CVE-2026-20096	6.5 MEDIUM
CVE-2026-20097	6.5 MEDIUM
CVE-2026-20087	4.8 MEDIUM
CVE-2026-20088	4.8 MEDIUM
CVE-2026-20089	4.8 MEDIUM
CVE-2026-20090	4.8 MEDIUM
CVE-2026-20085	6.1 MEDIUM

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CWE-787	Out-of-bounds Write

Getroffen producten

Cisco
Cisco Unified Computing System (Standalone)
Cisco Unified Computing System E-Series Software (UCSE)
Enterprise NFV Infrastructure Software
Integrated Management Controller

Disclaimer