Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0271

Kwetsbaarheid verholpen in Cisco Secure Firewall Management Center

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-09-2026
Revisie: 1.0.1

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

Update Revisie 1

New revision

Feiten

Cisco heeft een kwetsbaarheid verholpen in Cisco Secure Firewall Management Center.

Duiding

De kwetsbaarheid bevindt zich in de webinterface van Cisco Secure Firewall Management Center en betreft een hard-coded, statisch wachtwoord voor een laaggeprivilegieerd account. Hierdoor kunnen niet-geauthenticeerde externe aanvallers toegang verkrijgen zonder inloggegevens. Deze toegang kan leiden tot het blootstellen van gevoelige data die door het systeem wordt opgeslagen of beheerd. In combinatie met andere kwetsbaarheden kan deze toegang leiden tot privilege-escalatie.

Het Amerikaanse CISA heeft de kwetbaarheid op de Known Exploited Vulnerabilities-lijst geplaatst, wat indicatief is dat er binnen de Amerikaanse Federale Overheid misbruik heeft plaatsgevonden van deze kwetsbaarheid.

Het is goed gebruik om web-interfaces van management omgevingingen *niet* publiek toegankelijk te hebben, maar af te steunen in een separate beheer-omgeving.

UPDATE 11-09-26: Cisco meldt dat succesvolle exploitatie van de kwetsbaarheid met kenmerk CVE-2026-20316 is waargenomen. Organisaties wordt geadviseerd de updates van Cisco direct toe te passen en kwetsbare systemen te controleren op aanwijzingen van misbruik. Raadpleeg de Talos blog voor aanvullende aanbevelingen.
EINDE UPDATE

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://blog.talosintelligence.com/fmc-ongoing-exploitation
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-static-cred-BET3Cjh

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20316	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-259	Use of Hard-coded Password

Getroffen producten

Cisco
Cisco Secure Firewall Management Center (FMC)
Cisco Secure Firewall Management Center (FMC) Appliances

Disclaimer