



Advisory NCSC-2026-0458

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Cisco Secure Firewall ASA, Threat Defense en Management Center

Publicatiedatum: 28-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Cisco heeft kwetsbaarheden verholpen in Secure Firewall ASA, Threat Defense en Management Center softwareproducten. Cisco heeft de kwetsbaarheden gegroepeerd naar acht verschillende kwetsbaarheidsklassen (CWE's) en aan iedere groep één CVE-kenmerk toegekend.

Duiding

De kwetsbaarheden betreffen verschillende beveiligingsproblemen, waaronder onvoldoende toegangscontrole, onjuiste verwerking van invoergegevens, fouten in beveiligingsmechanismen en onjuiste afhandeling van uitzonderingssituaties. Vier van de acht CVE-registraties hebben een CVSS-score van 9.0 of hoger.

De kwetsbaarheden met kenmerk CVE-2026-20329 en CVE-2026-20330 hebben beide een CVSS-score van 9.9. Voor beide kwetsbaarheidsklassen geldt dat misbruik via het netwerk mogelijk is met beperkte gebruikersrechten en zonder gebruikersinteractie. De kwetsbaarheden met kenmerk CVE-2026-20331 en CVE-2026-20332 hebben respectievelijk een CVSS-score van 9.6 en 9.0 en betreffen tekortkomingen in beveiligingsmechanismen en toegangscontrole.

Cisco meldt dat twee kwetsbaarheden binnen de categorie toegangscontrole actief worden misbruikt. Het betreft de eerder afzonderlijk gepubliceerde kwetsbaarheden CVE-2026-20079 en CVE-2026-20316 in Cisco Secure FMC. De kwetsbaarheden kunnen respectievelijk leiden tot het omzeilen van authenticatie en het verkrijgen van toegang met statische inloggegevens. Het NCSC heeft voor deze kwetsbaarheden reeds advisories uitgebracht.

Voor de overige kwetsbaarheden uit deze hardeningrelease meldt Cisco geen bekend actief misbruik.

Oplossingen

Cisco heeft een hardening update uitgebracht om de kwetsbaarheden in Secure Firewall ASA, Threat Defense en Management Center te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-asaftdfmc-uvpPROhN>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20329	9.9 CRITICAL
CVE-2026-20330	9.9 CRITICAL
CVE-2026-20331	9.6 CRITICAL
CVE-2026-20332	9.9 CRITICAL
CVE-2026-20333	8.8 HIGH
CVE-2026-20334	8.4 HIGH
CVE-2026-20335	8.1 HIGH
CVE-2026-20336	8.8 HIGH

CWE's

CWE	Beschrijving
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-259	Use of Hard-coded Password

Getroffen producten

Cisco
Adaptive Security Appliance
Cisco Secure Firewall Management Center
Firepower Threat Defense

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 or 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.