



NCSC-2026-0076

Kwetsbaarheden verholpen in Cisco Secure Firewall Management Center

NCSC Advisory

PRIORITEIT: HOOG

Gepubliceerd op: 19-03-2026

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

Uit onderzoek van Amazon threat intelligence blijkt dat CVE-2026-20131 vermoedelijk al sinds 26 januari actief is misbruikt voor het uitrollen van Interlock ransomware.

Feiten

De kwetsbaarheid met kenmerk CVE-2026-20079 bevindt zich in de webinterface van Cisco Secure Firewall Management Center. Een ongeauthenticeerde externe kwaadwillende kan de authenticatiecontroles omzeilen door een onjuist systeemproces dat bij het opstarten is aangemaakt te misbruiken. De kwaadwillende kan deze kwetsbaarheid misbruiken door speciaal geprepareerde HTTP-verzoeken naar een getroffen apparaat te sturen. Een succesvolle exploit kan de aanvaller in staat stellen verschillende scripts en commando's uit te voeren die root-toegang tot het apparaat mogelijk maken.

De kwetsbaarheid met kenmerk CVE-2026-20131 bevindt zich in de webinterface van Cisco Secure Firewall Management Center. Deze kwetsbaarheid stelt ongeauthenticeerde externe kwaadwillende in staat om willekeurige Java-code uit te voeren met root-rechten. De kwetsbaarheid wordt veroorzaakt door de onveilige deserialisatie van door de gebruiker aangeleverde Java-byte-stromen. Een kwaadwillende kan deze kwetsbaarheid misbruiken door een speciaal geprepareerd, geserialiseerd Java-object naar de webgebaseerde beheerinterface van een getroffen apparaat te sturen. Een succesvolle exploit kan de aanvaller in staat stellen om willekeurige code op het apparaat uit te voeren en de rechten te verhogen tot root-niveau.

Als de beheerinterface van Cisco Secure Firewall Management Center geen publieke internettoegang heeft, wordt het aanvalsoppervlak verkleind. Het is niet gebruikelijk om een managementinterface direct publiekelijk aan het internet bloot te stellen.

Indien jouw organisatie gebruikmaakt van Cisco Security Cloud Control Firewall Management, dan betreft dit een SaaS-dienst (Software-as-a-Service) die door Cisco Systems automatisch wordt bijgewerkt als onderdeel van regulier onderhoud. Er is in dat geval geen actie van de gebruiker vereist.

Het NCSC verwacht op korte termijn een publieke PoC en grootschalige pogingen tot misbruik. Het NCSC adviseert met klem de update zo spoedig mogelijk te installeren.

Update 19-03-26:

Uit onderzoek van Amazon threat intelligence blijkt dat CVE-2026-20131 vermoedelijk al sinds 26 januari actief is misbruikt voor het uitrollen van Interlock ransomware. Daarnaast is er inmiddels een publieke PoC verschenen voor kwetsbaarheid CVE-2026-20079. Het is daarom van groot belang om - indien dit nog niet gedaan is - te updaten naar de nieuwste versie van Cisco Secure Firewall Management Center.

Duiding

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheden te verhelpen.

In een blog van Amazon worden onder andere IoC's en detectiemaatregelen gegeven om (pogingen tot) compromittatie op te sporen. Ook als de updates al snel na bekendmaking geïnstalleerd waren is het raadzaam om met behulp van de informatie uit het Amazon blog tot 26 januari terug te kijken op zoek naar verdacht netwerkverkeer en afwijkende handelingen op het systeem.

Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://aws.amazon.com/de/blogs/security/amazon-threat-intelligence-teams-identify-interlock-ransomware-campaign-targeting-enterprise-firewalls/>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-rce-NKhnULJh>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-onprem-fmc-authbypass-5Jp45V2>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-20079	10.0 CRITICAL
➤ CVE-2026-20131	10.0 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-288	Authentication Bypass Using an Alternate Path or Channel
➤ CWE-502	Deserialization of Untrusted Data

Getroffen producten

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

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 of 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.