



Advisory NCSC-2026-0450

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Snort 3 van Cisco

Publicatiedatum: 22-10-2026

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 meerdere kwetsbaarheden verholpen in Snort 3, het open source intrusion detection en prevention systeem dat in diverse Cisco-producten wordt gebruikt.

Duiding

De kwetsbaarheden bevinden zich in verschillende componenten van de Snort 3 Detection Engine, waaronder de SMTP MIME Decoder, NetFlow Detection Engine, GRE Detection Engine, Teredo Detection Engine, VBA Decompression Engine, en de memory management. Ongeauthenticeerde remote aanvallers kunnen speciaal vervaardigde pakketten of datagrammen versturen die leiden tot onverwachte herstarts van de detectie-engine, wat resulteert in een denial of service. Daarnaast is er een kwetsbaarheid in de control channel socket die een geauthenticeerde lokale aanvaller met lage privileges in staat stelt om arbitrary commands uit te voeren en toegang te krijgen tot het geheugen van het Snort 3 proces. De kwetsbaarheden beïnvloeden de stabiliteit, betrouwbaarheid en continuïteit van netwerkverkeersinspectie en dreigingsdetectie binnen de getroffen Cisco-producten.

Oplossingen

Cisco heeft updates en software hardening releases uitgebracht om deze kwetsbaarheden in Snort 3 te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-opensrc-snort3-2fXGJPfe>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-gre-JNpMHRtv>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-gtpcodec-dos-Rmecfepz>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-mime-vulns-bkXjcKkt>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-misc-dos-6mB22qAK>
- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort3-vba-bufdos-jAuFdvN9>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-20011	5.8 MEDIUM
CVE-2026-20019	5.8 MEDIUM
CVE-2026-20043	9.0 CRITICAL
CVE-2026-20179	5.8 MEDIUM
CVE-2026-20197	5.8 MEDIUM
CVE-2026-20218	5.8 MEDIUM
CVE-2026-20221	5.8 MEDIUM
CVE-2026-20236	7.5 HIGH
CVE-2026-20291	7.8 HIGH
CVE-2026-20356	7.5 HIGH
CVE-2026-76445	5.3 MEDIUM
CVE-2026-76489	5.8 MEDIUM
CVE-2026-76524	7.8 HIGH

CWE's

CWE	Beschrijving
CWE-121	Stack-based Buffer Overflow
CWE-128	Wrap-around Error
CWE-306	Missing Authentication for Critical Function
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-476	NULL Pointer Dereference
CWE-787	Out-of-bounds Write
CWE-805	Buffer Access with Incorrect Length Value
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')

Getroffen producten

Cisco
Cisco Cyber Vision
Cisco Firepower 1000 Series
Cisco Firepower 2100 Series
Cisco Open Source Snort3
Cisco Secure Firewall 4200 Series
Cisco Secure Firewall Threat Defense (FTD) Software
Cisco UTD SNORT IPS Engine Software
Cisco Umbrella Insights Virtual Appliance
Cyber Vision

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.