



Advisory NCSC-2026-0463

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in Cisco Secure Firewall ASA en FTD Software

Publicatiedatum: 30-10-2026

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 een ernstige kwetsbaarheid verholpen in Cisco Secure Firewall Adaptive Security Appliance (ASA) en Cisco Secure Firewall Threat Defense (FTD).

Duiding

Cisco bevestigt dat de kwetsbaarheid actief wordt misbruikt. Deze kwetsbaarheid met kenmerk CVE-2026-76418 heeft een CVSS-score van 8.6 en bevindt zich in de Remote Access SSL VPN-functionaliteit. Een niet-geauthenticeerde kwaadwillende kan de kwetsbaarheid op afstand misbruiken door een speciaal vervaardigd verzoek naar de VPN-dienst te versturen. Hierdoor kan het getroffen apparaat onverwacht herstarten, wat kan leiden tot een Denial-of-Service (DoS) en verstoring van de dienstverlening.

Voor succesvol misbruik moet de SSL VPN-dienst bereikbaar zijn en secundaire authenticatie zijn geconfigureerd voor een VPN-tunnelgroep. Een succesvolle VPN-aanmelding is niet vereist.

Oplossingen

Cisco heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Controleer of secundaire authenticatie is geconfigureerd voor VPN-tunnelgroepen. Cisco beschrijft tijdelijke mitigerende maatregelen, maar waarschuwt dat deze de beveiliging van VPN-toegang kunnen verlagen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-tunnel-dos-s6mgkb75>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-76418	8.6 HIGH

CWE's

CWE	Beschrijving
CWE-476	NULL Pointer Dereference

Getroffen producten

Cisco
Cisco Secure Firewall Adaptive Security Appliance (ASA) Software
Cisco Secure Firewall Threat Defense (FTD) Software
Secure Firewall ASA Software and Cisco Secure FTD Software

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.