



NCSC-2025-0373

Kwetsbaarheden verholpen in Fortinet FortiOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 19-11-2025

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

Feiten

Fortinet heeft kwetsbaarheden verholpen in FortiOS (meerdere versies).

Duiding

De kwetsbaarheden omvatten een stack-gebaseerde buffer overflow die aanvallers in staat stelt om ongeautoriseerde code of commando's uit te voeren door speciaal vervaardigde pakketten te verzenden. Een specifieke kwetsbaarheid in de FortiOS CAPWAP-daemon stelt een externe, niet-geauthenticeerde aanvaller op een aangrenzend netwerk in staat om deze pakketten te verzenden, mits de aanvaller controle heeft over een geautoriseerde FortiAP en zich op hetzelfde lokale IP-subnet bevindt. Daarnaast kunnen geauthenticeerde beheerders de trusted host policy omzeilen door op maat gemaakte CLI-commando's uit te voeren, wat kan leiden tot ongeautoriseerde toegang of acties binnen de getroffen omgevingen.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-25-358>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-545>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-632>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-53843	7.5 HIGH
➤ CVE-2025-54821	1.9 LOW
➤ CVE-2025-58413	7.5 HIGH

CWE's

CWE	Beschrijving
> CWE-121	Stack-based Buffer Overflow
> CWE-269	Improper Privilege Management

Getroffen producten

Fortinet
FortiOS

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.