Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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