



NCSC-2026-0015

Kwetsbaarheid verholpen in Fortinet FortiOS

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-09-2026

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

Aan deze advisory is toegevoegd dat deze kwetsbaarheid is opgenomen in de KEV-catalogus.

Feiten

Fortinet heeft een kwetsbaarheid verholpen in FortiOS (Specifiek voor FortiSASE en FortiSwitchManager).

Duiding

De kwetsbaarheid bevindt zich in de cw_acd daemon in FortiOS en FortiSwitchManager. Deze daemon is kwetsbaar voor exploitatie door externe, niet-geauthenticeerde aanvallers. Door het verzenden van speciaal vervaardigde pakketten of verzoeken, kunnen aanvallers willekeurige code of commando's op de getroffen systemen uitvoeren.

UPDATE Het Amerikaanse CISA heeft op 9 september de kwetsbaarheid op de Known Exploited Vulnerabilities-catalogus geplaatst. Organisaties wordt geadviseerd de updates van Fortinet direct toe te passen en kwetsbare, extern bereikbare systemen te controleren op aanwijzingen van misbruik. **EINDE UPDATE**

Oplossingen

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

Referenties

➤ <https://fortiguard.fortinet.com/psirt/FG-IR-25-084>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-25249	8.1 HIGH

CWE's

CWE	Beschrijving
➤ CWE-122	Heap-based Buffer Overflow

[CWE-787](#)

Out-of-bounds Write

Getroffen producten

Fortinet

FortiOS

FortiSwitchManager

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.