



# NCSC-2025-0192

## Kwetsbaarheden verholpen in Fortinet FortiOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-06-2025

**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](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

## Feiten

Fortinet heeft kwetsbaarheden verholpen in FortiOS.

## Duiding

De kwetsbaarheden omvatten onder andere een onjuiste certificaatvalidatie die het mogelijk maakt voor aanvallers om verbinding te maken met FortiClient via ingetrokken certificaten, wat leidt tot ongeautoriseerde toegang. Daarnaast zijn er kwetsbaarheden in de sessie-expiratie en privilegebeheer die aanvallers in staat stellen om ongeautoriseerde toegang te verkrijgen tot gevoelige instellingen en systemen. De exploitatie van deze kwetsbaarheden kan leiden tot gevolgen voor de integriteit van de netwerken en systemen die deze producten gebruiken.

## Oplossingen

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

## Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-23-008>
- <https://fortiguard.fortinet.com/psirt/FG-IR-23-342>
- <https://fortiguard.fortinet.com/psirt/FG-IR-23-375>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-058>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-257>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-339>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-365>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-544>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-006>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-287>

## Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-24471	6.5 MEDIUM
➤ CVE-2024-50562	4.8 MEDIUM
➤ CVE-2025-22862	6.7 MEDIUM

➤ CVE-2025-22254	6.6 MEDIUM
➤ CVE-2024-50568	5.9 MEDIUM
➤ CVE-2025-25250	4.3 MEDIUM
➤ CVE-2023-29184	3.2 LOW
➤ CVE-2025-22251	3.1 LOW
➤ CVE-2024-54019	4.8 MEDIUM
➤ CVE-2024-32119	4.8 MEDIUM
➤ CVE-2023-48786	4.3 MEDIUM

## CWE's

CWE	Beschrijving
➤ CVE-1390	Weak Authentication
➤ CVE-923	Improper Restriction of Communication Channel to Intended Endpoints
➤ CVE-297	Improper Validation of Certificate with Host Mismatch
➤ CVE-613	Insufficient Session Expiration
➤ CVE-300	Channel Accessible by Non-Endpoint
➤ CVE-295	Improper Certificate Validation
➤ CVE-459	Incomplete Cleanup
➤ CVE-918	Server-Side Request Forgery (SSRF)
➤ CVE-200	Exposure of Sensitive Information to an Unauthorized Actor
➤ CVE-269	Improper Privilege Management

## Getroffen producten

<b>Fortinet</b>
FortiOS
FortiProxy
FortiClientWindows
FortiClientEMS
FortiWeb
FortiSASE

## 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.