



# NCSC-2026-0061

## Kwetsbaarheden verholpen in Fortinet FortiOS

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-02-2026

**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 (Versies 7.0 tot 7.6.4, 7.4.0 tot 7.4.9, en 7.2.0 tot 7.2.11).

## Duiding

De kwetsbaarheden omvatten een Authentication Bypass die ongeauthenticeerde aanvallers in staat stelt om LDAP-authenticatie te omzeilen voor Agentless VPN of FSSO-beleid, afhankelijk van specifieke configuraties van de LDAP-server. Daarnaast kunnen ongeauthenticeerde aanvallers gevoelige informatie blootleggen door patches te omzeilen via speciaal gemaakte HTTP-verzoeken. Er is ook een kwetsbaarheid die geauthenticeerde beheerders in staat stelt om ongeautoriseerde code uit te voeren via speciaal gemaakte configuraties, en een andere die geauthenticeerde gebruikers in staat stelt om FSSO-beleid configuraties te exploiteren voor ongeautoriseerde toegang tot beschermde netwerkbronnen. Beide kwetsbaarheden kunnen worden misbruikt via speciaal gemaakte verzoeken.

## Oplossingen

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

## Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-25-1052>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-384>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-795>
- <https://fortiguard.fortinet.com/psirt/FG-IR-25-934>

## Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-22153	8.1 HIGH
➤ CVE-2025-68686	5.9 MEDIUM
➤ CVE-2025-64157	6.7 MEDIUM
➤ CVE-2025-62439	4.2 MEDIUM

## CWE's

CWE	Beschrijving
> <a href="#">CWE-134</a>	Use of Externally-Controlled Format String
> <a href="#">CWE-200</a>	Exposure of Sensitive Information to an Unauthorized Actor
> <a href="#">CWE-305</a>	Authentication Bypass by Primary Weakness
> <a href="#">CWE-940</a>	Improper Verification of Source of a Communication Channel

## 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.