



# NCSC-2024-0287

## Kwetsbaarheden verholpen in Fortinet

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 10-07-2024

### **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 een aantal kwetsbaarheden verholpen in FortiAIOPS, Fortinet FortiPortal, FortiWeb en Fortinet FortiExtender.

## Duiding

De meest serieuze kwetsbaarheden zijn CVE-2024-23663, CVE-2024-27782 en CVE-2024-27784. Welke in Fortinet FortiExtender en FortiAIOPS zitten.

Fortinet FortiExtender: Fortinet FortiExtender is een apparaat welke internet verbinding via 4g en 5g ondersteund. Een kwaadwillende kan de CVE-2024-23663 kwetsbaarheid die in Fortinet FortiExtender misbruiken om via HTTP verzoeken verhoogde rechten te krijgen.

FortiAIOPS (versie 2.0.0): De andere twee kwetsbaarheden, CVE-2024-27784 en CVE-2024-27782, zitten in FortiAIOPS versie 2.0.0. FortiAIOPS is een platform welke netwerk verkeer ondersteund door artificiële intelligentie en machine learning. Dit doet dit door diverse data stromen van het netwerk te integreren. Een kwaadwillende kan de CVE-2024-27782 kwetsbaarheid misbruiken om met gestolen sessie tokens ongeautoriseerde verzoeken in te dienen. Een kwaadwillende kan de CVE-2024-27784 kwetsbaarheid misbruiken, mits hij geauthenticeerd is tot FortiAIOPS, om gevoelige data in te zien van een API endpoint of log files.

## Oplossingen

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

## Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-22-326>
- <https://fortiguard.fortinet.com/psirt/FG-IR-23-459>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-011>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-069>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-072>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-073>
- <https://fortiguard.com/psirt/FG-IR-23-459>
- <https://fortiguard.fortinet.com/psirt/FG-IR-22-326>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-011>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-069>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-072>
- <https://fortiguard.fortinet.com/psirt/FG-IR-24-073>

## Kwetsbaarheden

CVE	CVSS Score
> CVE-2024-21759	4.3 MEDIUM
> CVE-2024-33509	4.8 MEDIUM
> CVE-2024-27782	8.1 HIGH
> CVE-2024-27784	8.8 HIGH
> CVE-2024-23663	8.8 HIGH
> CVE-2024-27785	5.4 MEDIUM

## CWE's

CWE	Beschrijving
> CVE-1236	Improper Neutralization of Formula Elements in a CSV File
> CVE-284	Improper Access Control
> CVE-295	Improper Certificate Validation
> CVE-532	Insertion of Sensitive Information into Log File
> CVE-613	Insufficient Session Expiration
> CVE-639	Authorization Bypass Through User-Controlled Key

## Getroffen producten

<b>fortinet</b>
fortiaio
fortiextender
fortiportal
fortiweb

## 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.