Nationaal Cyber Security Centrum
*Ministerie van Justitie en Veiligheid*

# NCSC-2025-0166

## Kwetsbaarheden verholpen in Fortinet producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 14-05-2025

**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 FortiManager, FortiManager Cloud, FortiAnalyzer, FortiOS, FortiProxy, FortiPAM, FortiSRA, FortiSwitchManager en FortiWeb.

## Duiding

De kwetsbaarheden omvatten een OS Command Injection die lokale aanvallers in staat stelt om ongeautoriseerde code uit te voeren door CLI-commando-argumenten te manipuleren. Daarnaast zijn er kwetsbaarheden die het mogelijk maken voor aanvallers om ongeautoriseerde wijzigingen aan te brengen in globale dreigingsfeeds en om authenticatie te omzeilen, wat leidt tot administratieve toegang tot de apparaten. Ook zijn er kwetsbaarheden die kunnen leiden tot denial-of-service door het versturen van speciaal vervaardigde verzoeken. Deze kwetsbaarheden kunnen leiden tot controle over de getroffen systemen.

## Oplossingen

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

## Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-24-325
- https://fortiguard.fortinet.com/psirt/FG-IR-24-381
- https://fortiguard.fortinet.com/psirt/FG-IR-24-388
- https://fortiguard.fortinet.com/psirt/FG-IR-23-167
- https://fortiguard.fortinet.com/psirt/FG-IR-23-490
- https://fortiguard.fortinet.com/psirt/FG-IR-25-122
- https://fortiguard.fortinet.com/psirt/FG-IR-24-472
- https://fortiguard.fortinet.com/psirt/FG-IR-24-023
- https://www.fortiguard.com/psirt/FG-IR-24-472

## Kwetsbaarheden

| CVE | CVSS Score |
| --- | --- |
| CVE-2023-42788 | 7.8 HIGH |
| CVE-2023-48795 | 6.0 MEDIUM |
| CVE-2024-6387 | |

| | |
|---|---|
| CVE-2024-45324 | 8.6 HIGH |
| CVE-2024-54020 | 2.3 LOW |
| CVE-2025-22252 | 9.8 CRITICAL |
| CVE-2025-26466 | 6.9 MEDIUM |
| CVE-2025-47294 | 5.3 MEDIUM |
| CVE-2025-47295 | 3.7 LOW |

## CWE's

| CWE | Beschrijving |
|---|---|
| CWE-222 | Truncation of Security-relevant Information |
| CWE-364 | Signal Handler Race Condition |
| CWE-134 | Use of Externally-Controlled Format String |
| CWE-354 | Improper Validation of Integrity Check Value |
| CWE-190 | Integer Overflow or Wraparound |
| CWE-362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition') |
| CWE-757 | Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade') |
| CWE-400 | Uncontrolled Resource Consumption |
| CWE-770 | Allocation of Resources Without Limits or Throttling |
| CWE-78 | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') |

## Getroffen producten

| **Fortinet** |
| --- |
| Fortinet<br>FortiOS |
| fortiproxy |
| Fortinet<br>FortiAnalyzer |
| Fortinet<br>FortiManager |
| FortiClient |
| FortiClient-<br>EMS |

## Disclaimer