



NCSC-2025-0018

Kwetsbaarheden verholpen in Fortinet FortiSwitch, FortiManager, FortiAnalyzer, FortiOS en FortiProxy

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 15-01-2025

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 FortiSwitch, FortiManager, FortiAnalyzer, FortiOS en FortiProxy.

Duiding

De kwetsbaarheden omvatten onder andere hard-coded cryptografische sleutels, onjuiste verwerking van OS-commando's, en out-of-bounds schrijf- en leesfouten. Aanvallers kunnen deze kwetsbaarheden misbruiken om ongeautoriseerde toegang te verkrijgen, willekeurige code uit te voeren en Denial-of-Service-aanvallen te veroorzaken.

Oplossingen

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

Referenties

- <https://www.fortiguard.com/psirt/FG-IR-24-239>
- <https://www.fortiguard.com/psirt/FG-IR-24-143>
- <https://www.fortiguard.com/psirt/FG-IR-24-097>
- <https://www.fortiguard.com/psirt/FG-IR-24-152>
- <https://www.fortiguard.com/psirt/FG-IR-24-222>
- <https://www.fortiguard.com/psirt/FG-IR-24-326>
- <https://www.fortiguard.com/psirt/FG-IR-24-282>
- <https://www.fortiguard.com/psirt/FG-IR-23-405>
- <https://www.fortiguard.com/psirt/FG-IR-23-260>
- <https://www.fortiguard.com/psirt/FG-IR-23-407>
- <https://www.fortiguard.com/psirt/FG-IR-24-267>
- <https://www.fortiguard.com/psirt/FG-IR-24-135>
- <https://www.fortiguard.com/psirt/FG-IR-24-219>
- <https://www.fortiguard.com/psirt/FG-IR-24-127>
- <https://www.fortiguard.com/psirt/FG-IR-23-293>
- <https://www.fortiguard.com/psirt/FG-IR-24-463>
- <https://www.fortiguard.com/psirt/FG-IR-24-061>
- <https://www.fortiguard.com/psirt/FG-IR-24-373>
- <https://www.fortiguard.com/psirt/FG-IR-24-259>
- <https://www.fortiguard.com/psirt/FG-IR-24-106>
- <https://www.fortiguard.com/psirt/FG-IR-23-258>
- <https://www.fortiguard.com/psirt/FG-IR-24-091>

- <https://www.fortiguard.com/psirt/FG-IR-23-473>
- <https://www.fortiguard.com/psirt/FG-IR-24-165>
- <https://www.fortiguard.com/psirt/FG-IR-24-250>
- <https://www.fortiguard.com/psirt/FG-IR-24-221>
- <https://www.fortiguard.com/psirt/FG-IR-23-494>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2022-23439	
➤ CVE-2023-37936	9.8 CRITICAL
➤ CVE-2023-37937	7.8 HIGH
➤ CVE-2023-42785	
➤ CVE-2023-42791	
➤ CVE-2023-46715	5.0 MEDIUM
➤ CVE-2024-21762	9.8 CRITICAL
➤ CVE-2024-26012	
➤ CVE-2024-27778	
➤ CVE-2024-32115	5.5 MEDIUM
➤ CVE-2024-33502	6.5 MEDIUM
➤ CVE-2024-33503	
➤ CVE-2024-35273	
➤ CVE-2024-35275	
➤ CVE-2024-35276	
➤ CVE-2024-35277	
➤ CVE-2024-36504	

> CVE-2024-36512	7.2 HIGH
> CVE-2024-46662	8.8 HIGH
> CVE-2024-46665	3.7 LOW
> CVE-2024-46666	
> CVE-2024-46668	
> CVE-2024-46669	
> CVE-2024-46670	7.5 HIGH
> CVE-2024-47571	8.1 HIGH
> CVE-2024-48884	7.5 HIGH
> CVE-2024-48886	9.0 CRITICAL
> CVE-2024-50566	
> CVE-2024-52963	3.7 LOW
> CVE-2024-54021	6.5 MEDIUM

CWE's

CWE	Beschrijving
> CVE-672	Operation on a Resource after Expiration or Release
> CVE-1390	Weak Authentication
> CVE-201	Insertion of Sensitive Information Into Sent Data
> CVE-266	Incorrect Privilege Assignment
> CVE-23	Relative Path Traversal
> CVE-190	Integer Overflow or Wraparound
> CVE-321	Use of Hard-coded Cryptographic Key
> CVE-125	Out-of-bounds Read

➤ CWE-306	Missing Authentication for Critical Function
➤ CWE-346	Origin Validation Error
➤ CWE-113	Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Request/Response Splitting')
➤ CWE-476	NULL Pointer Dereference
➤ CWE-770	Allocation of Resources Without Limits or Throttling
➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
➤ CWE-787	Out-of-bounds Write
➤ CWE-121	Stack-based Buffer Overflow
➤ CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

fortinet
fortiswitch
fortianalyzer
fortiproxy
fortios
fortimanager

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.