



NCSC-2026-0355

Kwetsbaarheden verholpen in Fortinet Forti-producten

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 09-09-2026

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Fortinet heeft kwetsbaarheden verholpen in FortiAnalyzer, FortiOS, FortiPAM, FortiProxy, FortiSandbox, FortiManager, FortiManager Cloud, FortiMonitorOnSight, FortiClient Windows, FortiSIEM en FortiSOAR.

Duiding

De kwetsbaarheden betreffen verschillende typen fouten in meerdere Fortinet-producten.

De ernstigste kwetsbaarheid met kenmerk CVE-2026-26084 heeft een CVSS-score van 8,9. Het betreft een autorisatiekwetsbaarheid in Fortinet FortiSandbox waardoor een ongeauthenticeerde kwaadwillende via speciaal vervaardigde HTTP-verzoeken toegang kan krijgen tot gevoelige informatie. De kwetsbaarheid vereist geen gebruikersinteractie en kan via het netwerk worden misbruikt.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheden in FortiOS, FortiPAM, FortiProxy, FortiAnalyzer, FortiSandbox, FortiMonitor en FortiManager te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-26-164>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-165>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-166>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-167>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-169>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-170>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-171>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-172>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-173>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-174>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-84391	6.5 MEDIUM
➤ CVE-2026-84392	2.7 LOW

➤ CVE-2026-26084	9.9 CRITICAL
➤ CVE-2026-84387	7.2 HIGH
➤ CVE-2026-22575	4.9 MEDIUM
➤ CVE-2026-84393	8.1 HIGH
➤ CVE-2026-84390	9.8 CRITICAL
➤ CVE-2026-84386	5.1 MEDIUM
➤ CVE-2026-84389	3.1 LOW
➤ CVE-2026-84385	5.4 MEDIUM

CWE's

CWE	Beschrijving
➤ CWE-77	Improper Neutralization of Special Elements used in a Command ('Command Injection')
➤ CWE-283	Unverified Ownership
➤ CWE-297	Improper Validation of Certificate with Host Mismatch
➤ CWE-457	Use of Uninitialized Variable
➤ CWE-476	NULL Pointer Dereference
➤ CWE-540	Inclusion of Sensitive Information in Source Code
➤ CWE-601	URL Redirection to Untrusted Site ('Open Redirect')

Getroffen producten

Fortinet
FortiAnalyzer
FortiClientWindows
FortiManager

FortiManager Cloud
FortiMonitor
FortiMonitor OnSight
FortiOS
FortiPAM
FortiProxy
FortiSIEM
FortiSOAR PaaS
FortiSOAR on- premise
FortiSandbox
FortiSandbox Cloud
FortiSandbox PaaS
Fortimonitor_Onsight
fortinet
FortiMonitorOnSight
FortiPAM Chrome Extension
FortiSOAR PaaS
FortiSandbox Cloud
FortiSandbox PaaS

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.