Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0488

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Fortinet FortiManager en FortiAnalyzer

Publicatiedatum: 12-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Fortinet heeft meerdere kwetsbaarheden verholpen in FortiManager en FortiAnalyzer, inclusief hun cloudversies en aanverwante producten zoals FortiManager Cloud, FortiAnalyzer Cloud, FortiAnalyzer-BigData, FortiSASE-Sovereign en FortiSASE-Sovereign GUI.

Duiding

De kwetsbaarheden betreffen diverse beveiligingsproblemen in Fortinet FortiManager en FortiAnalyzer producten, waaronder path traversal, improper encoding of escaping, extern gecontroleerde format string, SQL-injectie, XML-injectie, heap- en stack-based buffer overflows, OS command injection, privilege escalation, authorization bypass, argument injection, unrestricted file upload, server-side template injection, out-of-bounds write, en improper certificate validation binnen het RADIUS-protocol.

Deze kwetsbaarheden kunnen door een aanvaller worden misbruikt om, afhankelijk van de specifieke kwetsbaarheid, ongeautoriseerde code of commando's uit te voeren, bestanden te lezen, schrijven of verwijderen, privileges te escaleren, authenticatie te omzeilen, configuraties te manipuleren, en denial-of-service te veroorzaken. Sommige kwetsbaarheden vereisen authentificatie met verschillende privilege niveaus, variërend van read-only gebruikers tot geauthenticeerde beheerders, terwijl andere ook misbruikt kunnen worden door niet-geauthenticeerde aanvallers.

De kwetsbaarheden zijn aanwezig in zowel on-premises als cloudversies van de FortiManager en FortiAnalyzer producten en beïnvloeden belangrijke netwerkbeheer- en beveiligingsanalysefuncties. Exploitatie kan leiden tot compromittering van systeemintegriteit, controle over beheerde apparaten, en verstoring van netwerkbeheerprocessen. Specifieke aanvalsvectoren omvatten het verzenden van speciaal vervaardigde HTTP/HTTPS-requests, JSON-RPC-requests, OFTP-pakketten, en manipulatie van GUI-interfaces en template engines.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheden in FortiManager en FortiAnalyzer, inclusief hun cloudvarianten, te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-26-190
- https://fortiguard.fortinet.com/psirt/FG-IR-26-219
- https://fortiguard.fortinet.com/psirt/FG-IR-26-220
- https://fortiguard.fortinet.com/psirt/FG-IR-26-221
- https://fortiguard.fortinet.com/psirt/FG-IR-26-222
- https://fortiguard.fortinet.com/psirt/FG-IR-26-223
- https://fortiguard.fortinet.com/psirt/FG-IR-26-224
- https://fortiguard.fortinet.com/psirt/FG-IR-26-225
- https://fortiguard.fortinet.com/psirt/FG-IR-26-226
- https://fortiguard.fortinet.com/psirt/FG-IR-26-227
- https://fortiguard.fortinet.com/psirt/FG-IR-26-228
- https://fortiguard.fortinet.com/psirt/FG-IR-26-229
- https://fortiguard.fortinet.com/psirt/FG-IR-26-230
- https://fortiguard.fortinet.com/psirt/FG-IR-26-231
- https://fortiguard.fortinet.com/psirt/FG-IR-26-232
- https://fortiguard.fortinet.com/psirt/FG-IR-26-233
- https://fortiguard.fortinet.com/psirt/FG-IR-26-234
- https://fortiguard.fortinet.com/psirt/FG-IR-26-235
- https://fortiguard.fortinet.com/psirt/FG-IR-26-236
- https://fortiguard.fortinet.com/psirt/FG-IR-26-237
- https://fortiguard.fortinet.com/psirt/FG-IR-26-238
- https://fortiguard.fortinet.com/psirt/FG-IR-26-239
- https://fortiguard.fortinet.com/psirt/FG-IR-26-240
- https://fortiguard.fortinet.com/psirt/FG-IR-26-241
- https://fortiguard.fortinet.com/psirt/FG-IR-26-242
- https://fortiguard.fortinet.com/psirt/FG-IR-26-243
- https://fortiguard.fortinet.com/psirt/FG-IR-26-244
- https://fortiguard.fortinet.com/psirt/FG-IR-26-245
- https://fortiguard.fortinet.com/psirt/FG-IR-26-246
- https://fortiguard.fortinet.com/psirt/FG-IR-26-247
- https://fortiguard.fortinet.com/psirt/FG-IR-26-248
- https://fortiguard.fortinet.com/psirt/FG-IR-26-249
- https://fortiguard.fortinet.com/psirt/FG-IR-26-250
- https://fortiguard.fortinet.com/psirt/FG-IR-26-251

- https://fortiguard.fortinet.com/psirt/FG-IR-26-274
- https://fortiguard.fortinet.com/psirt/FG-IR-26-275
- https://fortiguard.fortinet.com/psirt/FG-IR-26-276

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-61625	8.1 HIGH
CVE-2026-126170	9.8 CRITICAL
CVE-2026-126171	7.2 HIGH
CVE-2026-126175	8.8 HIGH
CVE-2026-126176	8.1 HIGH
CVE-2026-126177	8.1 HIGH
CVE-2026-126178	7.2 HIGH
CVE-2026-126179	7.2 HIGH
CVE-2026-126180	8.4 HIGH
CVE-2026-126181	8.0 HIGH
CVE-2026-126182	7.2 HIGH
CVE-2026-126183	8.7 HIGH
CVE-2026-126184	8.2 HIGH
CVE-2026-126185	7.2 HIGH
CVE-2026-126211	7.2 HIGH
CVE-2026-126212	7.2 HIGH
CVE-2026-126213	7.1 HIGH
CVE-2026-126214	8.7 HIGH
CVE-2026-126215	8.7 HIGH
CVE-2026-126216	8.7 HIGH
CVE-2026-126217	8.7 HIGH
CVE-2026-126218	8.2 HIGH
CVE-2026-126219	7.2 HIGH

CVE	CVSS Score
CVE-2026-126220	7.2 HIGH
CVE-2026-126221	7.2 HIGH
CVE-2026-126222	7.2 HIGH
CVE-2026-126223	7.2 HIGH
CVE-2026-126224	7.2 HIGH
CVE-2026-126225	7.1 HIGH
CVE-2026-126226	7.2 HIGH
CVE-2026-126227	7.2 HIGH
CVE-2026-126228	7.2 HIGH
CVE-2026-126229	9.1 CRITICAL
CVE-2026-126230	7.2 HIGH
CVE-2026-126231	7.2 HIGH
CVE-2026-126232	7.5 HIGH
CVE-2026-126233	7.2 HIGH
CVE-2026-126234	7.2 HIGH
CVE-2026-126235	7.2 HIGH
CVE-2026-126236	7.2 HIGH
CVE-2026-126261	9.8 CRITICAL
CVE-2026-126262	9.8 CRITICAL
CVE-2026-126260	

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-88	Improper Neutralization of Argument Delimiters in a Command
CWE-89	Improper Neutralization of Special Elements used in an SQL Command

CWE	Beschrijving
CWE-91	XML Injection
CWE-94	Improper Control of Generation of Code
CWE-116	Improper Encoding or Escaping of Output
CWE-121	Stack-based Buffer Overflow
CWE-122	Heap-based Buffer Overflow
CWE-134	Use of Externally-Controlled Format String
CWE-290	Authentication Bypass by Spoofing
CWE-295	Improper Certificate Validation
CWE-434	Unrestricted Upload of File with Dangerous Type
CWE-441	Unintended Proxy or Intermediary
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-787	Out-of-bounds Write
CWE-798	Use of Hard-coded Credentials
CWE-862	Missing Authorization
CWE-863	Incorrect Authorization
CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine

Getroffen producten

Fortinet
FortiAnalyzer
FortiAnalyzer Cloud
FortiManager
FortiManager Cloud

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.