Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0086

Kwetsbaarheden verholpen in Fortinet FortiManager en FortiAnalyzer

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-03-2026

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 en FortiManager (inclusief cloudvarianten).

Duiding

De kwetsbaarheid met kenmerk CVE-2025-54820 zit in FortiManager. Deze kwetsbaarheid stelt een remote ongeauthenticeerde kwaadwillende in staat om via een stack-gebaseerde buffer overflow in de fgtupdates-service ongeautoriseerde commando's uit te voeren. Verder is er onder andere ook een kwetsbaarheid door onjuiste certificaatvalidatie die man-in-the-middle aanvallen mogelijk maakt, en een format string kwetsbaarheid die remote aanvallers met administratieve privileges in staat stelt om willekeurige code uit te voeren. Bovendien zijn er kwetsbaarheden in de multifactor authenticatie implementatie en in de beperking van overmatige authenticatiepogingen.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-26-078
- https://fortiguard.fortinet.com/psirt/FG-IR-26-079
- https://fortiguard.fortinet.com/psirt/FG-IR-26-081
- https://fortiguard.fortinet.com/psirt/FG-IR-26-090
- https://fortiguard.fortinet.com/psirt/FG-IR-26-092
- https://fortiguard.fortinet.com/psirt/FG-IR-26-095
- https://fortiguard.fortinet.com/psirt/FG-IR-26-098

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-48418	6.7 MEDIUM
CVE-2025-54820	8.1 HIGH
CVE-2025-68482	6.9 MEDIUM
CVE-2025-68648	7.2 HIGH

CVE-2026-22572	7.2 HIGH
CVE-2026-22629	3.7 LOW
CVE-2025-49784	6.0 MEDIUM

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-121	Stack-based Buffer Overflow
CWE-134	Use of Externally-Controlled Format String
CWE-288	Authentication Bypass Using an Alternate Path or Channel
CWE-295	Improper Certificate Validation
CWE-307	Improper Restriction of Excessive Authentication Attempts
CWE-912	Hidden Functionality

Getroffen producten

Fortinet
FortiAnalyzer
FortiAnalyzer Cloud
FortiManager
FortiManager Cloud

Disclaimer