Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0053

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

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 18-02-2025
Revisie: 1.0.1

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

Update Revisie 1

Actief misbruik waargenomen van CVE-2024-55591.

Feiten

Fortinet heeft kwetsbaarheden verholpen in verschillende producten, waaronder FortiOS, FortiProxy, FortiPAM, FortiSwitchManager, FortiSandbox, FortiManager en FortiAnalyzer.

Duiding

De kwetsbaarheden omvatten onder andere de mogelijkheid voor geprivilegieerde aanvallers om willekeurige code of commando's uit te voeren door het verzenden van speciaal vervaardigde verzoeken. Dit kan leiden tot ongeautoriseerde toegang en controle over de getroffen systemen. Daarnaast zijn er kwetsbaarheden gerapporteerd die het mogelijk maken voor geauthenticeerde gebruikers om gevoelige informatie te benaderen, zoals certificaat privé-sleutels en versleutelde wachtwoorden. Een kwetsbaarheid in FortiOS stelt aanvallers in staat om hun privileges te escaleren tot super-admin, wat risico's met zich meebrengt voor de integriteit van de systemen.

UPDATE: het NCSC heeft singalen ontvangen dat de kwetsbaarheid CVE-2024-55591 in FortiOS en Fortiproxy actief wordt misbruikt voor ransomware aanvallen. Er is (nog) geen publieke Proof-of-Concept (PoC) of exploit beschikbaar.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-24-094
- https://fortiguard.fortinet.com/psirt/FG-IR-24-160
- https://fortiguard.fortinet.com/psirt/FG-IR-24-302
- https://fortiguard.fortinet.com/psirt/FG-IR-24-220
- https://fortiguard.fortinet.com/psirt/FG-IR-24-147
- https://fortiguard.fortinet.com/psirt/FG-IR-24-063
- https://fortiguard.fortinet.com/psirt/FG-IR-24-311
- https://fortiguard.fortinet.com/psirt/FG-IR-23-261
- https://fortiguard.fortinet.com/psirt/FG-IR-24-422
- https://fortiguard.fortinet.com/psirt/FG-IR-24-535

Kwetsbaarheden

CVE	CVSS Score
CVE-2023-40721	6.7 MEDIUM
CVE-2024-27781	7.1 HIGH
CVE-2024-36508	6.0 MEDIUM
CVE-2024-40584	7.2 HIGH
CVE-2024-40585	6.5 MEDIUM
CVE-2024-40591	8.8 HIGH
CVE-2024-52966	2.3 LOW
CVE-2024-55591	9.8 CRITICAL
CVE-2025-24472	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-266	Incorrect Privilege Assignment
CWE-134	Use of Externally-Controlled Format String
CWE-288	Authentication Bypass Using an Alternate Path or Channel
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-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Getroffen producten

fortinet
fortianalyzer
fortimanager
fortios
fortios_and_fortiproxy
fortiswitchmanager

Disclaimer