Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0192

Kwetsbaarheden verholpen in Fortinet FortiOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 12-06-2025

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 FortiOS.

Duiding

De kwetsbaarheden omvatten onder andere een onjuiste certificaatvalidatie die het mogelijk maakt voor aanvallers om verbinding te maken met FortiClient via ingetrokken certificaten, wat leidt tot ongeautoriseerde toegang. Daarnaast zijn er kwetsbaarheden in de sessie-expiratie en privilegebeheer die aanvallers in staat stellen om ongeautoriseerde toegang te verkrijgen tot gevoelige instellingen en systemen. De exploitatie van deze kwetsbaarheden kan leiden tot gevolgen voor de integriteit van de netwerken en systemen die deze producten gebruiken.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-23-008
- https://fortiguard.fortinet.com/psirt/FG-IR-23-342
- https://fortiguard.fortinet.com/psirt/FG-IR-23-375
- https://fortiguard.fortinet.com/psirt/FG-IR-24-058
- https://fortiguard.fortinet.com/psirt/FG-IR-24-257
- https://fortiguard.fortinet.com/psirt/FG-IR-24-339
- https://fortiguard.fortinet.com/psirt/FG-IR-24-365
- https://fortiguard.fortinet.com/psirt/FG-IR-24-544
- https://fortiguard.fortinet.com/psirt/FG-IR-25-006
- https://fortiguard.fortinet.com/psirt/FG-IR-24-287

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-24471	**6.5 MEDIUM**
CVE-2024-50562	**4.8 MEDIUM**
CVE-2025-22862	**6.7 MEDIUM**

CVE-2025-22254	**6.6 MEDIUM**
CVE-2024-50568	**5.9 MEDIUM**
CVE-2025-25250	**4.3 MEDIUM**
CVE-2023-29184	**3.2 LOW**
CVE-2025-22251	**3.1 LOW**
CVE-2024-54019	**4.8 MEDIUM**
CVE-2024-32119	**4.8 MEDIUM**
CVE-2023-48786	**4.3 MEDIUM**

CWE's

CWE	Beschrijving
CWE-1390	Weak Authentication
CWE-923	Improper Restriction of Communication Channel to Intended Endpoints
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-613	Insufficient Session Expiration
CWE-300	Channel Accessible by Non-Endpoint
CWE-295	Improper Certificate Validation
CWE-459	Incomplete Cleanup
CWE-918	Server-Side Request Forgery (SSRF)
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-269	Improper Privilege Management

Getroffen producten

Fortinet
FortiOS
FortiProxy
FortiClientWindows
FortiClientEMS
FortiWeb
FortiSASE

Disclaimer