Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0386

Kwetsbaarheden verholpen in Fortinet producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 10-12-2025

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, FortiProxy, FortiWeb en FortiSwitchManager.

Duiding

De kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om toegang te krijgen tot de systemen door gebruik te maken van verschillende technieken, waaronder het omzeilen van FortiCloud SSO-login authenticatie via speciaal vervaardigde SAML-berichten, het behouden van actieve SSLVPN-sessies ondanks een wachtwoordwijziging, en het uitvoeren van ongeautoriseerde operaties via vervalste HTTP- of HTTPS-verzoeken. Dit kan leiden tot ongeautoriseerde toegang tot gevoelige API-gegevens en andere netwerkbronnen.

Oplossingen

Als mitigerende maatregel tegen de authenticatie-bypass kan FortiCloud SSO login worden uitgeschakeld. Fortinet heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-24-268
- https://fortiguard.fortinet.com/psirt/FG-IR-25-411
- https://fortiguard.fortinet.com/psirt/FG-IR-25-647
- https://fortiguard.fortinet.com/psirt/FG-IR-25-945
- https://fortiguard.fortinet.com/psirt/FG-IR-25-984

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-59718	9.8 CRITICAL
CVE-2025-59719	9.8 CRITICAL
CVE-2025-62631	5.6 MEDIUM
CVE-2024-47570	6.6 MEDIUM
CVE-2025-64471	4.9 MEDIUM

CVE-2025-64447	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-347	Improper Verification of Cryptographic Signature
CWE-532	Insertion of Sensitive Information into Log File
CWE-613	Insufficient Session Expiration

Getroffen producten

Fortinet
FortiOS
FortiProxy
FortiSwitchManager
FortiWeb

Disclaimer