Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0061

Kwetsbaarheden verholpen in Fortinet FortiOS

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 11-02-2026

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 FortiOS (Versies 7.0 tot 7.6.4, 7.4.0 tot 7.4.9, en 7.2.0 tot 7.2.11).

Duiding

De kwetsbaarheden omvatten een Authentication Bypass die ongeauthenticeerde aanvallers in staat stelt om LDAP-authenticatie te omzeilen voor Agentless VPN of FSSO-beleid, afhankelijk van specifieke configuraties van de LDAP-server. Daarnaast kunnen ongeauthenticeerde aanvallers gevoelige informatie blootleggen door patches te omzeilen via speciaal gemaakte HTTP-verzoeken. Er is ook een kwetsbaarheid die geauthenticeerde beheerders in staat stelt om ongeautoriseerde code uit te voeren via speciaal gemaakte configuraties, en een andere die geauthenticeerde gebruikers in staat stelt om FSSO-beleid configuraties te exploiteren voor ongeautoriseerde toegang tot beschermde netwerkbronnen. Beide kwetsbaarheden kunnen worden misbruikt via speciaal gemaakte verzoeken.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-25-1052
- https://fortiguard.fortinet.com/psirt/FG-IR-25-384
- https://fortiguard.fortinet.com/psirt/FG-IR-25-795
- https://fortiguard.fortinet.com/psirt/FG-IR-25-934

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-22153	8.1 HIGH
CVE-2025-68686	5.9 MEDIUM
CVE-2025-64157	6.7 MEDIUM
CVE-2025-62439	4.2 MEDIUM

CWE's

CWE	Beschrijving
CWE-134	Use of Externally-Controlled Format String
CWE-200	Exposure of Sensitive Information to an Unauthorized Actor
CWE-305	Authentication Bypass by Primary Weakness
CWE-940	Improper Verification of Source of a Communication Channel

Getroffen producten

Fortinet
FortiOS

Disclaimer