Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0372

Kwetsbaarheid verholpen in Fortinet FortiWeb

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 19-11-2025

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 een kwetsbaarheid verholpen in FortiWeb.

Duiding

De kwetsbaarheid bevindt zich in de wijze waarop Fortinet FortiWeb omgaat met HTTP-verzoeken en CLI-commando's. Geauthenticeerde aanvallers kunnen deze kwetsbaarheid misbruiken om ongeautoriseerde code uit te voeren via zorgvuldig samengestelde HTTP-verzoeken of CLI-commando's. Fortinet heeft bevestigd dat deze kwetsbaarheid actief wordt misbruikt. Er is (nog) geen publieke Proof-of-Concept-code (PoC) of exploit beschikbaar. Het NCSC verwacht dat PoC of Exploits op korte termijn beschikbaar komen, waarmee het risico op misbruik toeneemt.

Oplossingen

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

Versie	Geraakt	Oplossing
FortiWeb 8.0	8.00 tot 8.0.1	Upgrade naar 8.0.2 of hoger
FortiWeb 7.6	7.6.0 tot 7.6.5	Upgrade naar 7.6.6 of hoger
FortiWeb 7.4	7.4.0 tot 7.4.10	Upgrade naar 7.4.11 of hoger
FortiWeb 7.2	7.0.0 tot 7.0.11	Upgrade naar 7.0.12 of hoger

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-25-513
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog?field_cve=CVE-2025-58034

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-58034	7.2 HIGH

CWE's

CWE	Beschrijving
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Getroffen producten

Fortinet
FortiWeb

Disclaimer