Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2025-0255

Kwetsbaarheden verholpen in Fortinet producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-08-2025
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

CVE-2024-26009 toegevoegd

Feiten

Fortinet heeft kwetsbaarheden verholpen in FortiOS, FortiProxy, FortiPAM, FortiSIEM, FortiWeb en FortiADC.

Duiding

De meest ernstige kwetsbaarheid stelt een niet-geauthenticeerde aanvaller in staat om op afstand willekeurige code uit te voeren op FortiSIEM middels aangepaste CLI commando's. Forti geeft aan dat voor deze kwetsbaarheid PoC code beschikbaar is.

Daarnaast is er een kwetsbaarheid op FortiOS, FortiProxy en FortiPAM die een niet-geauthenticeerde aanvaller in staat stelt om de controle over een beheerd apparaat over te nemen via speciaal vervaardigde FGFM-verzoeken, als het apparaat wordt beheerd door een FortiManager en de aanvaller het serienummer van die FortiManager kent.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-24-364
- https://fortiguard.fortinet.com/psirt/FG-IR-25-152
- https://fortiguard.fortinet.com/psirt/FG-IR-25-173
- https://fortiguard.fortinet.com/psirt/FG-IR-25-253
- https://fortiguard.fortinet.com/psirt/FG-IR-25-383
- https://fortiguard.fortinet.com/psirt/FG-IR-25-448
- https://fortiguard.fortinet.com/psirt/FG-IR-25-501

Kwetsbaarheden

CVE	CVSS Score
CVE-2025-25248	5.3 MEDIUM
CVE-2025-25256	9.8 CRITICAL
CVE-2025-32766	6.4 MEDIUM
CVE-2025-47857	6.7 MEDIUM
CVE-2025-49813	7.2 HIGH
CVE-2025-52970	8.1 HIGH
CVE-2025-53744	7.2 HIGH
CVE-2024-26009	8.1 HIGH

CWE's

CWE	Beschrijving
CWE-266	Incorrect Privilege Assignment
CWE-190	Integer Overflow or Wraparound
CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
CWE-121	Stack-based Buffer Overflow
CWE-233	Improper Handling of Parameters

Getroffen producten

Fortinet
FortiADC
FortiOS

Disclaimer