



NCSC-2025-0226

Kwetsbaarheid verholpen in FortiWeb

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 11-07-2025

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

Er is een analyse verschenen waaruit Proof-of-Concept-Code (PoC) kan worden gemaakt. Een toename in pogingen tot misbruik wordt hiermee verwacht.

Feiten

Fortinet heeft een kwetsbaarheid verholpen in FortiWeb.

Duiding

De kwetsbaarheid stelt niet-geauthenticeerde aanvallers in staat om ongeautoriseerde SQL-commando's uit te voeren door speciaal vervaardigde HTTP-verzoeken te verzenden. Dit kan de integriteit en vertrouwelijkheid van de door FortiWeb beheerde gegevens in gevaar brengen.

Voor succesvol misbruik moet de kwaadwillende toegang hebben tot de HTTP Administrative interface. Het is goed gebruik een dergelijke interface niet publiek toegankelijk te hebben, maar af te steunen in een separaat beheer-lan.

Onderzoekers hebben een analyse gepubliceerd waarmee mogelijk werkende Proof-of-Concept-code kan worden geschreven. De werking is afhankelijk van de specifieke installatie, waardoor een universele PoC niet eenvoudig is te ontwikkelen. Het NCSC acht een toename in scanverkeer en pogingen tot misbruik wel waarschijnlijk. Hierom adviseert het NCSC om in elk geval de Administrative interface ontoegankelijk te maken vanaf externe netwerken, of deze, conform de door FortiNet geadviseerde mitigerende maatregel uit te schakelen.

Oplossingen

Fortinet heeft updates uitgebracht om de kwetsbaarheid te verhelpen. Als mitigerende maatregel adviseert FortiNet om de Administrative interface uit te schakelen. Zie bijgevoegde referenties voor meer informatie.

Referenties

➤ <https://www.fortiguard.com/psirt/FG-IR-25-151>

Kwetsbaarheden

CVE	CVSS Score

[> CVE-2025-25257](#)**9.8 CRITICAL**

CWE's

CWE	Beschrijving
> CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Getroffen producten

Fortinet
FortiWeb

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.