



NCSC-2026-0092

Kwetsbaarheden verholpen in Fortinet FortiWeb

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 12-03-2026

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 FortiWeb (Versies 7.0 tot 8.0.1).

Duiding

De kwetsbaarheden omvatten een mogelijkheid voor remote ongeauthenticeerde aanvallers om hostname-beperkingen te omzeilen, een OS command injection kwetsbaarheid binnen de FortiWeb API, en de mogelijkheid om authenticatie rate-limits te omzeilen. Daarnaast zijn er kwetsbaarheden gerapporteerd die leiden tot stack-based buffer overflows en een NULL Pointer Dereference, die kunnen worden misbruikt door geauthenticeerde aanvallers. Deze kwetsbaarheden kunnen resulteren in ongeautoriseerde toegang, uitvoering van willekeurige commando's, en verstoring van de beschikbaarheid van de FortiWeb service.

Oplossingen

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

Referenties

- <https://fortiguard.fortinet.com/psirt/FG-IR-26-082>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-087>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-088>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-089>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-093>
- <https://fortiguard.fortinet.com/psirt/FG-IR-26-097>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2025-48840	5.3 MEDIUM
➤ CVE-2025-66178	7.2 HIGH
➤ CVE-2026-24017	8.1 HIGH
➤ CVE-2026-24640	6.6 MEDIUM
➤ CVE-2026-24641	2.7 LOW

[> CVE-2026-30897](#)**6.6 MEDIUM**

CWE's

CWE	Beschrijving
> CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> CWE-121	Stack-based Buffer Overflow
> CWE-290	Authentication Bypass by Spoofing
> CWE-476	NULL Pointer Dereference
> CWE-799	Improper Control of Interaction Frequency

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.