Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0300

Kwetsbaarheden verholpen in Fortinet FortiWeb

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 13-08-2026

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.

Duiding

De eerste kwetsbaarheid betreft een Improper Authentication in meerdere versies van FortiWeb, waardoor een externe, niet-geauthenticeerde aanvaller toegang kan krijgen tot de GUI- en CLI-interfaces door het indienen van willekeurige inloggegevens. Deze kwetsbaarheid treedt ook op bij FortiWeb-systemen die zijn geconfigureerd met Remote Radius Type Admin Authentication onder bepaalde niet-standaard instellingen. Hierdoor kan een aanvaller de authenticatiemechanismen omzeilen zonder geldige credentials, wat mogelijk leidt tot het verkrijgen van administratieve controle over het apparaat. De tweede kwetsbaarheid betreft een onvolledige disallowed input list (CWE-184) in FortiWeb WAF, waardoor niet-geauthenticeerde aanvallers toegang kunnen krijgen door specifieke verzoeken te maken die de bedoelde inputrestricties omzeilen. Dit kan de effectiviteit van de WAF-beveiligingsregels ondermijnen en leiden tot ongeautoriseerde toegang of acties die de WAF juist moet voorkomen.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-26-157
- https://fortiguard.fortinet.com/psirt/FG-IR-26-158

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-26035	9.8 CRITICAL
CVE-2026-70466	5.3 MEDIUM

CWE's

CWE	Beschrijving
CWE-184	Incomplete List of Disallowed Inputs
CWE-287	Improper Authentication

Getroffen producten

Fortinet
FortiOS
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.