Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0490

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Fortinet FortiAuthenticator

Publicatiedatum: 12-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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 de-len. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Reacties zijn welkom op info@ncsc.nl.

Feiten

Fortinet heeft meerdere kwetsbaarheden verholpen in FortiAuthenticator versies 6.6.0 tot 6.6.10 en 8.0.0 tot 8.0.3.

Duiding

Meerdere kwetsbaarheden in FortiAuthenticator kunnen leiden tot ongeoorloofde toegang, informatielekken, code-uitvoering of uitval. Sommige zijn zonder account te misbruiken

- Open redirect: doorsturen van gebruikers naar ongewenste websites.
- Dienstverstoring: uitval door oneindige lussen of overbelasting.
- Toegangscontrole: ongeoorloofde toegang door fouten in autorisatie en rechtenbeheer.
- FSSO: buffer overflow in de authenticatieonderdelen.
- LDAP- en SQL-injectie: manipuleren van directory- en databaseopdrachten.
- Geheugenfouten: schrijven buiten geheugenbuffers en ongeldige geheugenverwijzingen.
- Formatstringfout: onveilige verwerking van aangeleverde tekst.
- Hardcoded wachtwoorden: misbruik van vaste, ingebouwde wachtwoorden.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-26-191
- https://fortiguard.fortinet.com/psirt/FG-IR-26-252
- https://fortiguard.fortinet.com/psirt/FG-IR-26-253
- https://fortiguard.fortinet.com/psirt/FG-IR-26-254
- https://fortiguard.fortinet.com/psirt/FG-IR-26-255
- https://fortiguard.fortinet.com/psirt/FG-IR-26-256
- https://fortiguard.fortinet.com/psirt/FG-IR-26-257
- https://fortiguard.fortinet.com/psirt/FG-IR-26-259

- https://fortiguard.fortinet.com/psirt/FG-IR-26-260
- https://fortiguard.fortinet.com/psirt/FG-IR-26-261
- https://fortiguard.fortinet.com/psirt/FG-IR-26-262
- https://fortiguard.fortinet.com/psirt/FG-IR-26-263
- https://fortiguard.fortinet.com/psirt/FG-IR-26-264
- https://fortiguard.fortinet.com/psirt/FG-IR-26-265
- https://fortiguard.fortinet.com/psirt/FG-IR-26-266
- https://fortiguard.fortinet.com/psirt/FG-IR-26-271

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-121526	6.1 MEDIUM
CVE-2026-126237	7.5 HIGH
CVE-2026-126238	8.6 HIGH
CVE-2026-126239	7.5 HIGH
CVE-2026-126240	8.2 HIGH
CVE-2026-126241	8.8 HIGH
CVE-2026-126242	7.4 HIGH
CVE-2026-126243	7.2 HIGH
CVE-2026-126244	7.5 HIGH
CVE-2026-126245	8.1 HIGH
CVE-2026-126246	7.5 HIGH
CVE-2026-126247	7.2 HIGH
CVE-2026-126248	7.5 HIGH
CVE-2026-126249	7.2 HIGH
CVE-2026-126250	8.2 HIGH
CVE-2026-126251	9.1 CRITICAL
CVE-2026-126252	8.3 HIGH
CVE-2026-126257	9.0 CRITICAL

CWE's

CWE	Beschrijving
CWE-89	Improper Neutralization of Special Elements used in an SQL Command
CWE-90	Improper Neutralization of Special Elements used in an LDAP Query
CWE-121	Stack-based Buffer Overflow
CWE-134	Use of Externally-Controlled Format String
CWE-259	Use of Hard-coded Password
CWE-476	NULL Pointer Dereference
CWE-522	Insufficiently Protected Credentials
CWE-601	URL Redirection to Untrusted Site
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-835	Loop with Unreachable Exit Condition
CWE-863	Incorrect Authorization

Getroffen producten

Fortinet
FortiAuthenticator

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.