Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0489

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Fortinet FortiOS

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 FortiOS.

Duiding

Verschillende kwetsbaarheden in FortiOS en andere Fortinet-producten kunnen leiden tot ongeoorloofde toegang, netwerkstoringen of volledige overname.

- SSLVPN: onderscheppen van verkeer door gebrekkige certificaatcontrole.
- Beheerinterface: verkrijgen van verhoogde rechten via een ongeldig token.
- OSPF: manipuleren van routinginformatie zonder in te loggen.
- iBGP: onverwacht routinggedrag door foutieve verwerking van gegevens.
- SSH: omzeilen van authenticatie met gemanipuleerde aanmeldgegevens.
- Geheugenfout: uitvoeren van code door een aanvaller met bestaande rechten.
- WAD: laten vastlopen van proxy- en ZTNA-verbindingen.
- HA FGSP: verkrijgen van volledige beheerderscontrole zonder account, bij bepaalde instellingen.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-26-193
- https://fortiguard.fortinet.com/psirt/FG-IR-26-195
- https://fortiguard.fortinet.com/psirt/FG-IR-26-267
- https://fortiguard.fortinet.com/psirt/FG-IR-26-268
- https://fortiguard.fortinet.com/psirt/FG-IR-26-269
- https://fortiguard.fortinet.com/psirt/FG-IR-26-270
- https://fortiguard.fortinet.com/psirt/FG-IR-26-272
- https://fortiguard.fortinet.com/psirt/FG-IR-26-273

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-121528	8.1 HIGH
CVE-2026-121530	6.6 MEDIUM
CVE-2026-126253	9.3 CRITICAL
CVE-2026-126254	9.6 CRITICAL
CVE-2026-126255	7.4 HIGH
CVE-2026-126256	7.4 HIGH
CVE-2026-126258	7.5 HIGH
CVE-2026-126259	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-24	Path Traversal: '../filedir'
CWE-121	Stack-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-197	Numeric Truncation Error
CWE-295	Improper Certificate Validation
CWE-305	Authentication Bypass by Primary Weakness
CWE-306	Missing Authentication for Critical Functionality

Getroffen producten

Fortinet
FortiOS

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.