Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0487

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Fortinet FortiMail

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 FortiMail.

Duiding

De kwetsbaarheden in FortiMail betreffen onder andere OS command injection, path traversal, SQL-injectie, authenticatie- en autorisatieproblemen, argument injection, XML-injectie, en resource consumptie. Sommige kwetsbaarheden kunnen door ongeauthenticeerde aanvallers worden misbruikt, terwijl andere authenticatie vereisen. Exploitatie kan leiden tot het uitvoeren van ongeautoriseerde commando's op root-niveau, het omzeilen van authenticatie en autorisatie, het resetten van wachtwoorden van webmailgebruikers, het lezen en verzenden van versleutelde e-mails namens andere gebruikers, het verwijderen van gebruikers in multi-tenant omgevingen, en het veroorzaken van denial-of-service door crashes of resource uitputting. De kwetsbaarheden beïnvloeden verschillende versies van FortiMail, met name versies tussen 7.2 en 8.0.2, en hebben impact op kernfunctionaliteiten zoals mailverwerking, webmailinterfaces, administratieve interfaces, en integratie met FortiAuthenticator.

Oplossingen

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

Referenties

- https://fortiguard.fortinet.com/psirt/FG-IR-26-196
- https://fortiguard.fortinet.com/psirt/FG-IR-26-197
- https://fortiguard.fortinet.com/psirt/FG-IR-26-198
- https://fortiguard.fortinet.com/psirt/FG-IR-26-199
- https://fortiguard.fortinet.com/psirt/FG-IR-26-200
- https://fortiguard.fortinet.com/psirt/FG-IR-26-201
- https://fortiguard.fortinet.com/psirt/FG-IR-26-202
- https://fortiguard.fortinet.com/psirt/FG-IR-26-203
- https://fortiguard.fortinet.com/psirt/FG-IR-26-204
- https://fortiguard.fortinet.com/psirt/FG-IR-26-205
- https://fortiguard.fortinet.com/psirt/FG-IR-26-206
- https://fortiguard.fortinet.com/psirt/FG-IR-26-207

- https://fortiguard.fortinet.com/psirt/FG-IR-26-208
- https://fortiguard.fortinet.com/psirt/FG-IR-26-209
- https://fortiguard.fortinet.com/psirt/FG-IR-26-210
- https://fortiguard.fortinet.com/psirt/FG-IR-26-211
- https://fortiguard.fortinet.com/psirt/FG-IR-26-212
- https://fortiguard.fortinet.com/psirt/FG-IR-26-213
- https://fortiguard.fortinet.com/psirt/FG-IR-26-214
- https://fortiguard.fortinet.com/psirt/FG-IR-26-215
- https://fortiguard.fortinet.com/psirt/FG-IR-26-216
- https://fortiguard.fortinet.com/psirt/FG-IR-26-217
- https://fortiguard.fortinet.com/psirt/FG-IR-26-218
- https://fortiguard.fortinet.com/psirt/FG-IR-26-277

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-126144	8.8 HIGH
CVE-2026-126145	7.2 HIGH
CVE-2026-126146	7.2 HIGH
CVE-2026-126147	9.8 CRITICAL
CVE-2026-126148	9.8 CRITICAL
CVE-2026-126149	7.5 HIGH
CVE-2026-126150	9.1 CRITICAL
CVE-2026-126151	7.5 HIGH
CVE-2026-126152	8.1 HIGH
CVE-2026-126153	7.5 HIGH
CVE-2026-126154	7.5 HIGH
CVE-2026-126155	9.1 CRITICAL
CVE-2026-126156	9.1 CRITICAL
CVE-2026-126157	9.1 CRITICAL
CVE-2026-126158	7.2 HIGH

CVE	CVSS Score
CVE-2026-126159	7.5 HIGH
CVE-2026-126160	8.2 HIGH
CVE-2026-126161	7.5 HIGH
CVE-2026-126162	8.7 HIGH
CVE-2026-126163	8.1 HIGH
CVE-2026-126164	9.4 CRITICAL
CVE-2026-126165	7.5 HIGH
CVE-2026-126166	7.6 HIGH
CVE-2026-126167	7.6 HIGH
CVE-2026-126168	7.6 HIGH
CVE-2026-126169	7.6 HIGH
CVE-2026-126263	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-88	Improper Neutralization of Argument Delimiters in a Command
CWE-89	Improper Neutralization of Special Elements used in an SQL Command
CWE-91	XML Injection
CWE-134	Use of Externally-Controlled Format String
CWE-190	Integer Overflow or Wraparound
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-639	Authorization Bypass Through User-Controlled Key
CWE-640	Weak Password Recovery Mechanism for Forgotten Password
CWE-787	Out-of-bounds Write
CWE-789	Memory Allocation with Excessive Size Value

CWE	Beschrijving
CWE-863	Incorrect Authorization

Getroffen producten

Fortinet
FortiMail

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.