



NCSC-2026-0398

Kwetsbaarheid verholpen in Fortinet FortiMail

NCSC Security Advisory

Prioriteit: Normaal

Gepubliceerd op: 02-10-2026

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 een kwetsbaarheid verholpen in FortiMail.

Duiding

FortiMail bevat een kritieke kwetsbaarheid (CVE-2026-104286) in de verwerking van bestandspaden, veroorzaakt door een combinatie van Path Traversal (CWE-22) en onvoldoende neutralisatie van NULL-bytes (CWE-158). Een niet-geauthenticeerde aanvaller kan via speciaal vervaardigde HTTP- of HTTPS-verzoeken willekeurige bestanden op het onderliggende systeem schrijven. De kwetsbaarheid wordt actief geëxploiteerd. Getroffen zijn FortiMail 7.2.0–7.2.9, 7.4.0–7.4.8, 7.6.0–7.6.6 en 8.0.0–8.0.1 waarbij de functionaliteit IBE (Identity Based Encryption) is aangezet. Deze functionaliteit maakt versleuteling naar derden mogelijk zonder dat zij over bekende certificaten beschikken.

Fortinet heeft Indicators of Compromise (IoC's) beschikbaar gesteld waarmee organisaties kunnen onderzoeken of er mogelijk misbruik van de kwetsbaarheid heeft plaatsgevonden. Gezien de actieve exploitatie van FortiMail is het raadzaam om naast het installeren van de beveiligingsupdate ook onderzoek uit te voeren naar mogelijke compromittering. Hierbij kunnen de door Fortinet gepubliceerde IoC's worden gebruikt als onderdeel van de forensische controle.

Oplossingen

Fortinet heeft beveiligingsupdates uitgebracht om de kwetsbaarheid te verhelpen. Daarnaast heeft Fortinet IoC's uitgebracht die kunnen helpen bij onderzoek en additionele mitigerende maatregelen benoemd in de FG-IR-26-175 advisory. Zie bijgevoegde referenties voor meer informatie.

Dreigingsinformatie

Indicators of Compromise (IoC): Files:

- [ADDED]/data/lib/liblog.so MD5 - 64c90a00c7fda4d5c7973ed64c25783a SHA256 - 8015f34dc84922b03688399d7f9fe7a00361789f7e420c7e2a2cdb23e75cef84
- [MODIFIED]/bin/smit MD5 - 5241738a3e9988404239e12243f6d35b SHA256 - 77324ac428bde86d351fc5fc06f6d64a6bfe737dfb2743df1d4c5ac2418a5b6a
- [ADDED]/data/bin/webconsole MD5 - ae0ea6502d3fa5f0664bceb73189eb54 SHA256 - 7a6cea9f5c9e2e9994d4e3c4da73f86cf5acd05ea5d312c066c9d1dafd69ee38
- [ADDED]/data/bin/mailservice MD5 - f90fa81a5f521d785f2b2f765e3ab897 SHA256 - 4000276a150a165d3c2537d1e19fb393c4de8333076a16655e28059cae82157b
- [MODIFIED]/data/etc/httpd.conf MD5 - 61af1c4bce1c2eebc8ff689ca5337791 SHA256 - 703e97c64e61e41dc3aaba580d82bb2aa7b6a11b54ee6fb467ed5d5a3bffdef5

- [ADDED]/data/etc/ld.so.preload MD5 - 8eb64f25d2a8e18e05aae058629473cf SHA256 - 8953ec7960b09f544a880b072ad4e6cfda7a8303f486251d3478dcdfbac23b6
- [MODIFIED] /data/migadmin.tar.gz MD5 - 49a7156a7d043cc8f9f680579db22f86 SHA256 - d6fe51c22b91776f4c961ea58bcac5917f15d560a619d7ce726d3d51795609d3 IPs:

79[.]141.169.187 45[.]129.0.192 Logs:

- type=event subtype=system pri=debug user=system ui=cron msg="(root) CMD (/bin/sh -c 'O=/migadmin ...
- type=kevent subtype=admin pri=information user=admin ui=(null) action=logout status=success reason=unknown msg="User admin logged out from (null)."
- type=kevent subtype=config pri=information user=admin ui=cli module=unknown submodule=unknown msg="Added 'archive234' to 'archive account' : rotation-size[50]rotation-time[1] rotation-hour[14]destination[remote]remote-ip[79.141.169.187]remote-username[archive234]remote-password[***]remote-directory[/uploads] (user: admin, from: cli)"
- FortiMail::IBE::DecrypterMediaIn::DecrypterMediaIn(FortiMail::MediaIn&, const FortiMail::IBE::KeyFinder&, const FortiMail::EmailAddress&, const FortiMail::Buffer&, FortiMail::IBE::DecrypterMediaIn::Version): Caught BufferException(2), BufferImpl.cpp:973, 'Invalid Base64 Encoding at pos 0. Character=0x2a'
- Internal user *@domain.tldmailto:*@domain.tld failed to log in.

Referenties

➤ <https://fortiguard.fortinet.com/psirt/FG-IR-26-175>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2026-104286	9.8 CRITICAL

CWE's

CWE	Beschrijving
➤ CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
➤ CWE-158	Improper Neutralization of Null Byte or NUL Character

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.