AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-104286

Path Traversal in FortiMail-IBE: Mail-Gateway ohne Anmeldung übernehmbar.

Die Funktion Identity-Based Encryption (IBE) von FortiMail prüft Dateipfade in HTTP-Anfragen unzureichend: Mit Verzeichniswechseln und eingeschleusten NULL-Bytes kann ein Angreifer ohne Anmeldung beliebige Dateien auf das Mail-Gateway schreiben – und damit eigenen Code ausführen. Fortinet hat die Lücke am 1. Oktober 2026 als bereits ausgenutzten Zero-Day gemeldet; am selben Tag hat CISA sie in den Katalog aktiv ausgenutzter Schwachstellen aufgenommen – mit forensischer Triage-Pflicht. Seit dem 5. Oktober stehen die korrigierten Versionen 8.0.2, 7.6.7 und 7.4.9 bereit; bis zum Update schützt nur der Workaround.

Geschäftsrisiko: vollständige Übernahme des Mail-Gateways mit Zugriff auf ein- und ausgehende E-Mails, Zugangsdaten und verbundene Verzeichnisdienste – als Ausgangspunkt für Business-E-Mail-Compromise, Datenabfluss und Erpressung; ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO ist in diesem Fall wahrscheinlich.

9,8 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz, ohne Rechte, ohne Zutun eines Nutzers, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Der Basiswert 9,8 stammt von Fortinet als CNA und wird von der NVD übernommen; Fortinet weist inklusive Temporal-Metriken (E:P/RL:O/RC:C) einen funktionsfähigen Exploit aus.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
spätestens 01.10.2026 (Zero-Day)	FortiMail 7.2.0 – 8.0.1 Fix: 8.0.2 · 7.6.7 · 7.4.9	Sofort

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Basiswert (Fortinet / NVD)

Path Traversal
IBE · NULL-Byte · Dateischreiben

Aktiv
ausgenutzt · CISA KEV · Frist 04.10.2026

Patch da
8.0.2 · 7.6.7 · 7.4.9 · Workaround bis Update

Die Ursache: FortiMail verarbeitet über die Webschnittstelle der Funktion **Identity-Based Encryption** (IBE) Anfragen, die Dateipfade enthalten. Die Prüfung, ob diese Pfade im vorgesehenen Verzeichnis bleiben, lässt sich mit Verzeichniswechseln (`../`, **CWE-22**) und eingeschleusten NULL-Bytes (**CWE-158**) aushebeln. Ein Angreifer kann so **ohne Zugangsdaten und ohne Nutzerinteraktion** beliebige Dateien auf das zugrunde liegende System schreiben – etwa Bibliotheken, Programme oder Konfigurationsdateien des Webservers – und erreicht damit Codeausführung auf dem Gateway. Erreichbar ist die Lücke überall dort, wo IBE aktiv und die Weboberfläche aus dem Internet zugänglich ist.

ANGRIFFSKETTE

01
IBE erreichbar – Webschnittstelle mit aktivierter Identity-Based Encryption im Internet

02
Präparierte Anfrage – Pfad mit ../ und NULL-Byte hebelt die Verzeichnisprüfung aus

03
Datei geschrieben – Bibliotheken, Binaries oder Webserver-Konfiguration ersetzt

04
Codeausführung – Kontrolle über das Gateway, Zugriff auf E-Mails und Zugänge

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiMail 8.0	`8.0.0 – 8.0.1`	8.0.2
FortiMail 7.6	`7.6.0 – 7.6.6`	7.6.7
FortiMail 7.4	`7.4.0 – 7.4.8`	7.4.9
FortiMail 7.2	`7.2.0 – 7.2.9`	Migration auf Zweig 7.4 oder höher

Fortinet hat die korrigierten Versionen **8.0.2 / 7.6.7 / 7.4.9** mit dem Advisory-Update vom 05.10.2026 („Solution update“) nachgereicht. Für Zweig 7.2 gibt es keinen eigenen Fix – Migration auf 7.4 oder höher. Der maschinenlesbare CVE-Record weicht bei Versionsgrenzen und Fixständen vom Advisory-Text ab – maßgeblich ist FG-IR-26-175. Bis zum Update bleibt der Workaround (IBE abschalten bzw. Weboberfläche abschotten) Pflicht.

Regulatorischer Hinweis: Ein übernommenes Mail-Gateway mit Zugriff auf Postfachinhalte ist in der Regel eine meldepflichtige Verletzung – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung, Forensik und Dokumentation.

ZEITACHSE

vor 01.10.2026
Ausnutzung als Zero-Day in freier Wildbahn

01.10.2026
Fortinet veröffentlicht FG-IR-26-175 mit Workaround

01.10.2026
Aufnahme in CISA-KEV · Frist 04.10.2026

05.10.2026
Fixversionen 8.0.2 / 7.6.7 / 7.4.9 erschienen

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Workaround sofort, Patch zügig, Prüfung vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
IBE abschalten oder Webzugriff sperren	Auf 8.0.2 / 7.6.7 / 7.4.9 aktualisieren	Kompromittierung ausschließen

01 Betroffenheit feststellen

Firmware-Stand aller FortiMail-Instanzen erheben (betroffen: 7.2.0 bis 8.0.1) und prüfen, ob IBE aktiv und die Weboberfläche aus dem Internet erreichbar ist. Trifft beides zu, ist die Instanz unmittelbar angreifbar.

02 Sofort mitigieren (vor dem Patch)

IBE deaktivieren – das ist der von Fortinet dokumentierte Workaround. Wird IBE fachlich benötigt, den Webzugriff aus dem Internet sperren bzw. auf vertrauenswürdige Netze beschränken und vorgeschaltet per WAF POST-Anfragen an `/ibe` mit Verzeichniswechseln blockieren.

```
config system encryption ibe · set
status disable · end
```

03 Patchen

Auf die korrigierten Versionen `8.0.2` · `7.6.7` · `7.4.9` aktualisieren; für Zweig 7.2 gibt es keinen eigenen Fix – Migration auf 7.4 oder höher einplanen. Vorher Konfigurationssicherung ziehen.

04 Kompromittierung ausschließen

Der Patch schließt die Tür – er wirft niemanden hinaus, der schon drin ist. Nach unbekannten Dateien unter `/data/bin/` und `/data/lib/`, veränderter `httpd.conf` und einer `ld.so.preload` suchen, Logs auf die IoCs prüfen, neue Archivkonten kontrollieren. CISA verlangt hier eine forensische Triage.

05 Bei Verdacht: Zugänge und Postfächer als offengelegt behandeln

Admin-, Dienst- und LDAP-Zugänge erneuern, Zertifikate tauschen, Archiv- und Weiterleitungsregeln prüfen – und Beweise sichern, bevor das Gerät neu aufgesetzt wird.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-IP-ADRESSEN

`79.141.169.187`
`45.129.0.192`

DATEIARTEFAKTE

Fremde Dateien in `/data/bin/` und `/data/lib/`
Veränderte `httpd.conf`, neue `ld.so.preload`

LOG-HINWEISE

POST-Anfragen an `/ibe` mit `../`
Archivkonten mit Remote-IP 79.141.169.187,
Base64-Dekodierfehler in IBE-Logs

Zur Einordnung: Die IP-Adressen und Log-Hinweise stammen aus dem Fortinet-Advisory, die Dateipfade aus Analysen von Sicherheitsdienstleistern (u. a. Truesec). Infrastruktur und Dateinamen sind trivial änderbar – belastbarer als die Suche nach einzelnen Indikatoren ist die Frage, ob IBE auf dem Gerät aus dem Internet erreichbar war.

Wichtig: Ein Angriff über IBE hinterlässt keinen Anmeldevorgang. Wer nur Authentifizierungs-Ereignisse überwacht, sieht die Übernahme nicht – ein Patch allein beweist nicht, dass niemand drin ist.

Bildmotive: KI-generierte Symbolbilder

Lassen Sie das von unseren Experten prüfen.

Drei Bausteine, die genau auf diese Schwachstelle einzahlen – vom schnellen Exposure-Check bis zur laufenden Absicherung.

Cyber Defense Center

Worauf wir bei dieser Schwachstelle achten: Unerwartete Dateiänderungen und Prozesse auf dem Mail-Gateway sowie neue Archiv- oder Weiterleitungsregeln ohne Change. Das setzt voraus, dass die nötigen Logquellen angebunden sind.

Vulnerability & Exposure Management

Wir finden aus dem Internet erreichbare FortiMail-Instanzen mit aktivierter Identity-Based Encryption über Ihren gesamten Perimeter – bevor Angreifer sie finden – und priorisieren nach realer Ausnutzung.

Incident-Response-Retainer

Bei Verdacht auf einen bereits erfolgten Zugriff übernimmt unser IR-Team Forensik und Eindämmung – mit vertraglich zugesicherter Reaktionszeit.

SO GEHEN WIR VOR

01 Exposure-Check

Wir prüfen, ob Ihre FortiMail-Systeme verwundbar konfiguriert und exponiert sind.

02 Sofortmaßnahmen begleiten

Mitigation und Patch-Fahrplan gemeinsam mit Ihrem Team umgesetzt.

03 Absichern & überwachen

Threat Hunting auf die IoCs, danach laufendes Monitoring und IR-Bereitschaft – 24/7, wenn Ihr Team das nicht selbst leisten kann.

Empfehlung für die Geschäftsleitung

- Heute anordnen: IBE abschalten oder den Webzugriff auf FortiMail aus dem Internet sperren, bis das Update eingespielt ist.
- Für jede FortiMail-Instanz mit erreichbarem IBE eine forensische Prüfung beauftragen – dokumentiert für eine etwaige Meldung.
- Fixversion zügig einspielen; Geräte auf Zweig 7.2 als Migrationsprojekt aufsetzen.

Ihr Part · unser Part. **Sie behalten die Kontrolle über Konfiguration und Freigaben; wir liefern Analyse, Bewertung und – im Retainer – die Reaktionskette.**

Rollen, Eingriffstiefe und SLAs im Erstgespräch (RACI, AVV/TOM auf Anfrage) · Datenhaltung auf Wunsch in Deutschland · ISO/IEC 27001 (TÜV SÜD) · deutschsprachige Analysten.

Sprechen Sie mit uns, bevor es ein Angreifer tut.

Kostenloses 30-Minuten-Erstgespräch – wir prüfen Ihre Exposure gegenüber CVE-2026-104286 und dem FortiMail-Perimeter.

+49 89 45 24 24-100 · kontakt@argos.security · www.argos.security

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Fortinet PSIRT Advisory FG-IR-26-175 · CVE-Record CVE-2026-104286 (Fortinet als CNA) · NVD CVE-2026-104286 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 01.10.2026) · Truesec, Analyse zu CVE-2026-104286 · watchTowr, FAQ zu CVE-2026-104286. Angaben nach bestem Wissen zum Stand 12.10.2026 (FG-IR-26-175, letzte Revision 07.10.2026) – gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.