THREAT INTELLIGENCE BRIEFING

CVE-2026-126147

# Codeausführung über die API von FortiMail.

Die API des E-Mail-Gateways FortiMail prüft Pfadangaben nicht ausreichend (Path Traversal). Ein Angreifer ohne Anmeldung kann dadurch mit präparierten Anfragen Code oder Befehle ausführen. Fortinet hat die Lücke am 10.11.2026 mit 8.0.2, 7.6.7 und 7.4.9 geschlossen; für den Zweig 7.2 gibt es keinen Fix, nur die Migration. Eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Übernahme des E-Mail-Gateways – mit Zugriff auf den gesamten Mailverkehr, einem Einstiegspunkt ins Firmennetz und einem meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

**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 Anmeldung, ohne Mitwirkung eines Nutzers, mit voller Wirkung auf das System. Basiswert laut NVD (Vektor von Fortinet als CNA); das Fortinet-Advisory nennt ebenfalls 9,8.

**AUSNUTZUNG**
Nicht bekannt (Stand 11.11.2026)

**BETROFFEN**
FortiMail 8.0.0–8.0.1, 7.6.0–7.6.6
7.4.0–7.4.8, 7.2 alle Versionen

**HANDLUNGSBEDARF**
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

# Das Wichtigste in 60 Sekunden.

**9,8 · KRITISCH**
CVSS-Schweregrad

**Ohne Anmeldung**
API · CWE-22

**Nicht bekannt**
Ausnutzung · nicht in CISA KEV · kein PoC öffentlich

**8.0.2 · 7.6.7 · 7.4.9**
Fixversionen seit 10.11.2026 · 7.2 migrieren

**Die Ursache:** Die betroffene Komponente ist laut Fortinet die **API von FortiMail**. Sie begrenzt Pfadangaben nicht zuverlässig auf das vorgesehene Verzeichnis (**CWE-22, Path Traversal**). Ein **nicht authentifizierter Angreifer** kann so über präparierte Anfragen nicht autorisierten Code oder Befehle ausführen. Fortinet hat die Lücke intern gefunden und nennt keine weiteren technischen Details.

## ANGRIFFSKETTE

01
**API erreichbar** – die FortiMail-API ist aus dem Netz ansprechbar

02
**Präparierte Anfrage** – Angreifer sendet Anfragen mit manipulierten Pfadangaben, ohne Anmeldung

03
**Verzeichnis verlassen** – Pfad wird nicht auf das erlaubte Verzeichnis begrenzt

04
**Codeausführung** – Befehle auf dem E-Mail-Gateway, Zugriff auf den Mailverkehr

## Betroffenheit & Fixversionen

| Produkt · Zweig | Verwundbar bis | Fixversion (Ziel) |
|---|---|---|
| FortiMail 8.0 | 8.0.0 bis 8.0.1 | 8.0.2 |
| FortiMail 7.6 | 7.6.0 bis 7.6.6 | 7.6.7 |
| FortiMail 7.4 | 7.4.0 bis 7.4.8 | 7.4.9 |
| FortiMail 7.2 | alle Versionen | Migration auf einen behobenen Zweig |

Angaben laut Fortinet-Advisory FG-IR-26-199. Fortinet nennt **keinen Workaround** und keinen virtuellen Patch. Für FortiMail 7.2 gibt es keine Fixversion – nur die Migration auf einen behobenen Zweig. FortiMail Cloud wurde laut Fortinet bereits am 05.10.2026 behoben; Cloud-Kunden müssen nichts tun.

**Regulatorischer Hinweis:** Ein bestätigter unbefugter Zugriff auf das E-Mail-Gateway kann eine meldepflichtige Verletzung darstellen – DSGVO unverzüglich (i. d. R. 72 h), NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

## ZEITACHSE

**05.10.2026**
FortiMail Cloud behoben

**10.11.2026**
FG-IR-26-199 · Fix 8.0.2 / 7.6.7 / 7.4.9

**11.11.2026**
CVE im NVD veröffentlicht

**Stand heute**
Nicht in CISA KEV · kein PoC



Bildmotive: KI-generierte Symbolbilder

# Ihr Maßnahmenplan.

In dieser Reihenfolge – Erreichbarkeit vor Patch, Patch vor Entwarnung.

| SOFORT | KURZFRISTIG | PARALLEL |
|---|---|---|
| API-Zugriff begrenzen | Update einspielen | Logs prüfen |

## 01 Betroffenheit feststellen

Version aller FortiMail-Instanzen prüfen: `8.0.0`–`8.0.1`, `7.6.0`–`7.6.6`, `7.4.0`–`7.4.8` und alle `7.2`-Versionen sind betroffen. Klären, von wo die Verwaltungs- und API-Schnittstelle erreichbar ist.

## 02 Patchen

Auf `8.0.2`, `7.6.7` bzw. `7.4.9` oder neuer aktualisieren. Systeme auf `7.2` auf einen behobenen Zweig migrieren. Vorher ein Konfigurations-Backup sichern.

## 03 Risiko bis zum Update senken

Fortinet nennt keinen Workaround. Den Zugriff auf Verwaltung und API per Firewall-Regel auf bekannte Admin-Netze beschränken, nie für das gesamte Internet öffnen.

## 04 Kompromittierung ausschließen

Logs auf ungewöhnliche API-Anfragen, unbekannte Admin-Konten und unerwartete Konfigurationsänderungen prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

## Kompromittierungs-Indikatoren (IoCs)

**ÖFFENTLICHE IOCS**

Keine – Fortinet nennt keine, Ausnutzung nicht bekannt

**AUSWERTUNGSQUELLEN**

FortiMail-Event- und Admin-Logs
Firewall- und Proxy-Logs zur Verwaltungsschnittstelle

**AUFFÄLLIGE MUSTER**

API-Anfragen mit Pfadsequenzen wie `../`
unerwartete Konten, Dateien oder Konfigurationsänderungen

**Zur Einordnung:** Es liegen keine CVE-spezifischen Indikatoren vor. Die genannten Muster sind Ansatzpunkte für eine Auswertung, keine bestätigten Signaturen.

**Wichtig:** FortiMail sieht den gesamten ein- und ausgehenden Mailverkehr. Wer das Gateway übernimmt, kann Mails mitlesen, manipulieren und von dort ins Netz vordringen.



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

24/7-SOC aus München: Eine API-Anfrage an FortiMail mit Pfadsequenzen von einer unbekannten Adresse fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

### Vulnerability & Exposure Management

Wir finden Aus dem Internet erreichbare FortiMail-Verwaltung 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

- Update aller FortiMail-Instanzen auf die Fixversionen anordnen – 7.2-Systeme migrieren.
- Bestätigen lassen, dass Verwaltung und API nicht offen im Internet stehen.
- Über eine dauerhafte Überwachung des E-Mail-Gateways entscheiden.

**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 vollständig 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-2026-126147 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 FG-IR-26-199 (10.11.2026, Fixversionen, CVSS 9,8) · NVD (CVSS 3.1 Basiswert 9,8, Quelle Fortinet als CNA) · CISA KEV (Stand 11.11.2026: nicht gelistet). Stand 11.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.