AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-32756

Pre-Auth-RCE per Stack-Overflow in mehreren Fortinet-Produkten.

Ein nicht authentifizierter Angreifer aus dem Internet kann über eine speziell gebaute Hash-Cookie in HTTP-Anfragen einen Stack-Überlauf in der Administrations-API auslösen und beliebigen Code ausführen – ohne gültige Anmeldedaten. Betroffen ist eine ganze Produktfamilie (FortiVoice, FortiMail, FortiNDR, FortiRecorder, FortiCamera); für FortiVoice ist die Ausnutzung als Zero-Day seit Mai 2025 bestätigt.

> **Geschäftsrisiko:** vollständige Übernahme des betroffenen Systems – mit Potenzial für Abgriff von Zugangsdaten, Persistenz im Netz, Sabotage der Kommunikations-/Sicherheitsinfrastruktur und einen 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 Rechte, ohne Zutun – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD-Basiswert 9,8 (CVSS 3.1, von Fortinet zugeteilt); Fortinet nennt im eigenen Advisory inkl. Temporal-Metriken 9,6. Eine CVSS-4.0-Bewertung liegt beim NVD nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Mai 2025	FortiVoice · FortiMail · FortiNDR FortiRecorder · FortiCamera	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Pre-Auth-RCE
Stack-Overflow in der Admin-API

Aktiv
ausgenutzt · CISA KEV · FortiVoice-Zero-Day

5 Produkte
betroffen · HTTP/HTTPS-Interface

Die Ursache: Die administrative Web-API der betroffenen Geräte kopiert den Wert einer speziell präparierten Hash-Cookie aus einer HTTP-Anfrage in einen Puffer fester Größe auf dem Stack, ohne die Länge zu prüfen (Stack-based Buffer Overflow, `CWE-121`). Ein Angreifer überschreibt damit gezielt den Stack und lenkt den Programmfluss auf eigenen Code – ohne Anmeldung, allein durch das Senden einer HTTP-Anfrage an das erreichbare Management-/Portal-Interface. Ergebnis ist eine Codeausführung mit den Rechten des Web-Dienstes.

ANGRIFFSKETTE

01
Interface exponiert – das HTTP/HTTPS-Administrations- oder Portal-Interface ist aus dem Internet erreichbar

02
Cookie präparieren – eine überlange, speziell gebaute `hash`-Cookie wird in einer HTTP-Anfrage gesendet

03
Stack überlaufen – der ungeprüfte Wert überschreibt den Stack und übernimmt den Programmfluss (`CWE-121`)

04
Code ausführen – Netzwerk-Scans, Löschen der Crashlogs, Aktivieren von `fcgi debugging` zum Mitschneiden von Zugangsdaten, Malware/Cron-Jobs

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiVoice 7.2	`7.2.0`	`7.2.1`
FortiVoice 7.0	`7.0.0 – 7.0.6`	`7.0.7`
FortiVoice 6.4	`6.4.0 – 6.4.10`	`6.4.11`
FortiMail 7.6	`7.6.0 – 7.6.2`	`7.6.3`
FortiMail 7.4	`7.4.0 – 7.4.4`	`7.4.5`
FortiMail 7.2	`7.2.0 – 7.2.7`	`7.2.8`
FortiMail 7.0	`7.0.0 – 7.0.8`	`7.0.9`
FortiNDR 7.6	`7.6.0`	`7.6.1`
FortiNDR 7.4	`7.4.0 – 7.4.7`	`7.4.8`
FortiNDR 7.2	`7.2.0 – 7.2.4`	`7.2.5`
FortiNDR 7.0	`7.0.0 – 7.0.6`	`7.0.7`

Ihr Maßnahmenplan.

In dieser Reihenfolge – Interface abschotten vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Inventar auf alle fünf Produktfamilien prüfen: FortiVoice, FortiMail, FortiNDR, FortiRecorder, FortiCamera. Version und Zweig gegen die Tabelle abgleichen. Ist das HTTP/HTTPS-Administrations- oder Portal-Interface aus dem Internet bzw. aus nicht vertrauenswürdigen Netzen erreichbar? Nur exponierte Interfaces sind praktisch angreifbar.

02 Sofort mitigieren (vor dem Patch)

Herstellerbehelf: das HTTP/HTTPS-Administrations- und Portal-Interface deaktivieren bzw. am exponierten Interface aus `allowaccess` entfernen und auf vertrauenswürdige Hosts / VPN beschränken:

```
config system interface edit <port> set allowaccess ping ssh next end
```

03 Patchen

Auf die Fixversion des jeweiligen Produkt-Zweigs aktualisieren (z. B. `FortiVoice 7.0.7` · `FortiMail 7.6.3` · `FortiNDR 7.4.8` · `FortiRecorder 7.2.4` · `FortiCamera 2.1.4`). Für FortiCamera 2.0 / 1.1 gibt es keinen In-Zweig-Fix – auf einen gepatchten Release migrieren.

04 Kompromittierung ausschließen

Auf die von Fortinet genannten Angreifer-Handlungen prüfen: aktiviertes `fcgi debugging` (ist standardmäßig aus), gelöschte System-Crashlogs, unbekannte Cron-Jobs, neue lokale Konten sowie die Quell-IPs unten. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter härten

Grundsatz durchsetzen: Administrations- und Portal-Interfaces nie direkt exponieren. Vorgelagerte WAF-/IPS-Signaturen für diese Schwachstelle einspielen, sofern verfügbar, und die Erreichbarkeit der gesamten Fortinet-Produktfamilie regelmäßig von außen kontrollieren.

Kompromittierungs-Indikatoren (IoCs)

ANGREIFER-QUELL-IPS

`198.105.127.124` · `43.228.217.173` `43.228.217.82` · `156.236.76.90` `218.187.69.244` · `218.187.69.59`

SYSTEMSEITIGE MARKER

aktiviertes `fcgi debugging` (Standard: aus) · gelöschte System-Crashlogs · unbekannte `cron`-Jobs zum Abgriff von Zugangsdaten

AKTIVITÄTSMUSTER

Netzwerk-Scans vom Gerät aus · Mitschnitt von SSH-/Login-Zugangsdaten · nachgeladene Malware

Zur Einordnung: Die Quell-IPs sind eine Momentaufnahme der von Fortinet beobachteten Kampagne und flüchtig – kein Ersatz für die Analyse Ihrer System- und Zugriffslogs. Das erneute Aktivieren von fcgi debugging und fehlende Crashlogs sind starke Indizien, aber kein Beweis; im Verdachtsfall das Gerät forensisch bewerten.

Wichtig: Eine erfolgreiche Ausnutzung führt zu Codeausführung auf dem Gerät. Beobachtet wurden Löschen der Crashlogs, Aktivieren von fcgi debugging zum Mitschneiden von Zugangsdaten und Cron-Jobs zur Persistenz – ein reiner Patch entfernt weder abgeflossene Zugangsdaten noch bereits gesetzte Persistenz. Ohne Prüfung des Systems bleibt eine erfolgte Kompromittierung unsichtbar.

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: Das nachträgliche Aktivieren von fcgi debugging, fehlende Crashlogs und anomale HTTP-Anfragen mit überlanger hash-Cookie fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte Fortinet-Management-/Portal-Interfaces (FortiVoice, FortiMail, FortiNDR, FortiRecorder, FortiCamera) 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 FortiVoice u. a.-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

- HTTP/HTTPS-Interfaces der betroffenen Fortinet-Systeme heute vom Internet trennen, Patch innerhalb der CISA-Frist (04.06.2025) bzw. umgehend einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist (fcgi debugging, Crashlogs, Cron-Jobs) – dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: Administrations- und Portal-Interfaces nie direkt exponieren.

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-2025-32756 und dem FortiVoice u. a.-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-25-254 (CVE-2025-32756, CVSS 9,6 inkl. Temporal) · NVD (nvd.nist.gov, CVSS 3.1 Basiswert 9,8, CWE-121/CWE-787) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 14.05.2025, Frist 04.06.2025). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Produkt-Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.