AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-39808

Befehlsausführung über die FortiSandbox-Programmierschnittstelle.

Über einen Schnittstellen-Aufruf der FortiSandbox kann ein Angreifer ohne Anmeldung eigene Betriebssystem-Befehle ausführen. Ein Proof-of-Concept liegt seit der Veröffentlichung im April 2026 öffentlich auf GitHub; seit dem 12. Juni 2026 werden Angriffsversuche beobachtet. CISA hat die Schwachstelle am 16.07.2026 in den Katalog aktiv ausgenutzter Schwachstellen aufgenommen.

> **Geschäftsrisiko:** vollständige Kontrolle über die Malware-Analyse-Plattform – mit Zugriff auf alle dort untersuchten Dateien, der Möglichkeit, Analyse-Ergebnisse zu fälschen, und einem Ausgangspunkt für Bewegungen im internen Netz. Ein bestätigter Zugriff kann ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO sein.

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 des Nutzers, mit vollem Verlust von Vertraulichkeit, Integrität und Verfügbarkeit. Das FortiGuard-Advisory FG-IR-26-100 weist denselben Sachverhalt mit 9,1 aus – beide Werte liegen im Bereich KRITISCH.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
12. Juni 2026	FortiSandbox 4.4.0 – 4.4.8 Fix: 4.4.9	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (NVD)

Unauth. RCE
über einen API-Aufruf

PoC öffentlich
seit April 2026 · CISA KEV 16.07.2026

4.4.9
schließt die Lücke

Die Ursache: Eine Programmierschnittstelle der FortiSandbox übergibt einen Wert aus der HTTP-Anfrage an einen Betriebssystem-Aufruf, ohne Sonderzeichen zu neutralisieren (CWE-78). Wer die Schnittstelle über das Netz erreicht, hängt an einen regulären Parameter eigene Kommandos an – **ohne Anmeldung** und mit den Rechten des ausführenden Dienstes. Anders als bei vielen Perimeter-Lücken existiert hier bereits seit der Veröffentlichung ein öffentlich abrufbarer Exploit.

ANGRIFFSKETTE

01 **Schnittstelle erreichbar** – FortiSandbox-API aus einem nicht vertrauenswürdigen Netz aufrufbar

02 **Parameter manipulieren** – Shell-Sonderzeichen an einen regulären API-Parameter anhängen

03 **Befehl ausführen** – das System führt die untergeschobenen Kommandos aus

04 **Zugriff verfestigen** – Analyse-Daten abgreifen, Ergebnisse manipulieren, weiter ins Netz

Betroffenheit & Fixversionen

FortiSandbox-Zweig	Verwundbar bis	Fixversion (Ziel)
4.4 (Appliance)	`4.4.0 – 4.4.8`	`4.4.9`
5.0 (Appliance)	nicht betroffen	—
PaaS 5.0	nicht betroffen	—
PaaS (ältere Builds)	21.3.4055 – 23.4.4374 (NVD)	Stand mit Fortinet abstimmen

Das Hersteller-Advisory FG-IR-26-100 führt ausschließlich den 4.4-Zweig als betroffen; die NVD-Produktliste nennt zusätzlich ältere PaaS-Builds (`21.3.4055-23.4.4374`). Für gehostete Instanzen deshalb den Versionsstand aktiv beim Hersteller erfragen statt aus der Advisory-Tabelle abzuleiten. Exakte Build-Stände immer gegen FG-IR-26-100 prüfen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf ein System, das Datei-Anhänge und Schadcode-Proben verarbeitet, 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

14.04.2026
Fortinet veröffentlicht FG-IR-26-100 (Fix 4.4.9)

April 2026
Proof-of-Concept öffentlich auf GitHub verfügbar

12.06.2026
Erste Angriffsversuche beobachtet (KEVIntel)

16.07.2026
Aufnahme in den CISA-KEV-Katalog · Frist 19.07.2026

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Version aller FortiSandbox-Systeme erheben. Betroffen ist der Zweig `4.4.0-4.4.8`; der 5.0-Zweig ist nach Herstellerangabe nicht betroffen. Für gehostete PaaS-Instanzen den Build-Stand beim Hersteller erfragen – die NVD-Liste nennt dort abweichende ältere Stände.

02 Erreichbarkeit sofort einschränken

Web-Oberfläche und Programmierschnittstelle gehören nicht ins Internet. Zugriff auf ein dediziertes Management-Netz oder Sprungsysteme mit Mehr-Faktor-Anmeldung begrenzen. Weil ein funktionsfähiger Exploit öffentlich verfügbar ist, ist die Netzabschottung hier die einzig wirksame Sofortmaßnahme – Fortinet nennt keinen Workaround.

03 Patchen

Auf `4.4.9` oder höher aktualisieren. Wer ohnehin einen Versionswechsel plant: Der 5.0-Zweig ist von dieser Schwachstelle nicht betroffen – wohl aber von CVE-2026-25089, dort ist `5.0.6` die Fixversion. Beide Advisories zusammen einplanen.

04 Kompromittierung ausschließen

API- und Web-Zugriffs-Logs auf Anfragen mit Shell-Sonderzeichen in Parametern durchsuchen, dazu neue oder veränderte Konten, geänderte Systemkonfiguration und unerwartete ausgehende Verbindungen. Bei öffentlich verfügbarem Exploit und beobachteten Angriffen ist der Zeitraum ab April 2026 zu betrachten – nicht erst ab der KEV-Aufnahme.

05 Integrität der Analyse-Ergebnisse bewerten

Wurde das System kompromittiert, sind auch dessen Urteile über geprüfte Dateien nicht mehr belastbar. In diesem Fall Analysen des betroffenen Zeitraums nachbewerten und die Sandbox erst nach Neuaufsetzen bzw. verifiziertem Patch wieder als Entscheidungsgrundlage nutzen.

Kompromittierungs-Indikatoren (IoCs)

WO SUCHEN

API- und Web-Zugriffs-Logs
HTTPS/443 – Aufrufe ohne vorherige Anmeldung

AUFFÄLLIGE MUSTER

Shell-Sonderzeichen in Anfrage-Parametern
`|` `;` `&` `$(` `)` `` ` `` · ungewöhnlich lange Parameterwerte

FOLGESPUREN

neue/veränderte Konten · geänderte Systemkonfiguration
unerwartete ausgehende Verbindungen vom Sandbox-System

Zur Einordnung: Fortinet hat zu dieser Schwachstelle keine IP-Adressen oder Signaturen veröffentlicht. Zum betroffenen Endpunkt kursieren öffentlich technische Analysen; wir führen hier bewusst nur die vom Hersteller und aus der Log-Praxis belastbaren Suchhinweise. Sie sind kein abschließender Nachweis und kein Ersatz für eine forensische Prüfung bei konkretem Verdacht.

Wichtig: Der öffentliche Proof-of-Concept liegt seit April 2026 vor – der relevante Prüfzeitraum beginnt also mit der Veröffentlichung, nicht mit der KEV-Aufnahme im Juli. Wer nur „seit letzter Woche" in die Logs schaut, sieht die entscheidenden Monate nicht.

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: Unauthentifizierte API-Aufrufe mit Shell-Sonderzeichen und anomale Prozess- oder Netzaktivität des Analyse-Systems fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden erreichbare, ungepatchte FortiSandbox-Systeme im 4.4-Zweig 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 FortiSandbox-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

- Erreichbarkeit von Oberfläche und Schnittstelle heute einschränken, Patch auf 4.4.9 kurzfristig einplanen.
- Rückblickende Prüfung ab April 2026 beauftragen – der Exploit ist seit der Veröffentlichung öffentlich.
- Beide FortiSandbox-Advisories (CVE-2026-39808 und CVE-2026-25089) in einem Wartungsfenster abarbeiten.

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-2026-39808 und dem FortiSandbox-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-26-100 · NVD CVE-2026-39808 · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 16.07.2026, Frist 19.07.2026) · Berichte zu beobachteten Angriffsversuchen (KEVIntel, Defused). Angaben nach bestem Wissen zum Stand 27.07.2026; Fixversionen und Build-Stände gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.