AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-25089

Unauthentifizierte Befehlsausführung in Fortinet FortiSandbox.

Ein Angreifer ohne jede Anmeldung kann über speziell gebaute HTTP-Anfragen an die Web-Oberfläche von FortiSandbox Betriebssystem-Befehle ausführen. Betroffen sind Appliance, Cloud und PaaS. CISA hat die Schwachstelle am 16.07.2026 in den Katalog aktiv ausgenutzter Schwachstellen aufgenommen – mit Umsetzungsfrist 19.07.2026 für US-Bundesbehörden.

> **Geschäftsrisiko:** vollständige Übernahme der Malware-Analyse-Plattform – und damit Einblick in alle dort untersuchten Dateien und Anhänge sowie ein Brückenkopf in ein besonders vertrauenswürdiges Segment Ihres Netzes. 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-26-141 weist denselben Sachverhalt mit 9,1 aus – beide Werte liegen im Bereich KRITISCH.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Juni 2026	FortiSandbox 4.2 / 4.4 / 5.0 + Cloud & PaaS 5.0	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (NVD)

Unauth. RCE
Web-Oberfläche · HTTPS/443

Aktiv
ausgenutzt · CISA KEV seit 16.07.2026

5.2-Zweig
und PaaS 23.4 nicht betroffen

Die Ursache: Die Web-Oberfläche von FortiSandbox übergibt Inhalte aus einer JSON-Eingabe der „Start VNC"-Funktion an einen Betriebssystem-Aufruf, ohne Sonderzeichen zu neutralisieren (CWE-78, Second-Order OS Command Injection). Wer den Dienst über das Netz erreicht, kann so **ohne gültige Anmeldedaten** eigene Befehle auf dem System ausführen lassen – über HTTP-Anfragen, die für die Anwendung wie regulärer Verkehr aussehen.

ANGRIFFSKETTE

01 **Oberfläche erreichbar** – FortiSandbox-Web-UI (443) aus einem nicht vertrauenswürdigen Netz aufrufbar

02 **Anfrage präparieren** – Sonderzeichen in der JSON-Eingabe der VNC-Funktion

03 **Befehl ausführen** – das System führt untergeschobene Kommandos aus, ohne Anmeldung

04 **Zugriff verfestigen** – Analyse-Daten abgreifen, Konfiguration ändern, weiter ins Netz

Betroffenheit & Fixversionen

FortiSandbox-Zweig	Verwundbar bis	Fixversion (Ziel)
5.0 (Appliance)	5.0.0 – 5.0.5	5.0.6
4.4 (Appliance)	4.4.0 – 4.4.8	4.4.9
4.2 (Appliance)	alle Versionen	Migration auf 4.4.9 / 5.0.6
Cloud 5.0	5.0.4 – 5.0.5	5.0.6
PaaS 5.0	5.0.4 – 5.0.5	5.0.6
5.2 · Cloud 5.2/4.4 · PaaS 23.4/5.2/4.4	nicht betroffen	—

Für den 4.2-Zweig nennt das Hersteller-Advisory keine eigene Fixversion – hier ist ein Wechsel auf einen gepflegten Zweig der Weg. Cloud- und PaaS-Instanzen aktualisiert Fortinet nicht automatisch für Sie: Version und Rollout-Stand aktiv mit dem Hersteller abgleichen. Exakte Build-Stände immer gegen FG-IR-26-141 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

09.06.2026
Fortinet veröffentlicht FG-IR-26-141 (Fix 4.4.9 / 5.0.6)

Juni 2026
Erste Angriffsversuche berichtet (Defused) – Exploit-Code zunächst fehlerhaft

16.07.2026
Aufnahme in den CISA-KEV-Katalog

19.07.2026
CISA-Umsetzungsfrist für US-Bundesbehörden abgelaufen

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
Management-Zugang abschotten	Patch einspielen	Log-Auswertung / Threat Hunting

01 Betroffenheit feststellen

Version aller FortiSandbox-Systeme erheben – Appliance, Cloud und PaaS getrennt. Betroffen sind `4.2` (alle), `4.4.0`-`4.4.8`, `5.0.0`-`5.0.5` sowie Cloud/PaaS `5.0.4`-`5.0.5`. Der 5.2-Zweig ist nach Herstellerangabe nicht betroffen.

02 Erreichbarkeit sofort einschränken

Die Web-Oberfläche (HTTPS/443) gehört nicht ins Internet. Zugriff auf ein dediziertes Management-Netz oder Sprungsysteme mit Mehr-Faktor-Anmeldung begrenzen – das ist die wirksame Sofortmaßnahme, solange der Patch aussteht. Fortinet nennt für diese Schwachstelle keinen dedizierten Workaround.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren: `4.4.9` bzw. `5.0.6` oder höher. Für den 4.2-Zweig existiert kein Fix – hier ist die Migration auf einen gepflegten Zweig einzuplanen.

04 Kompromittierung ausschließen

Zugriffs-Logs der Web-Oberfläche auf unerwartete Anfragen an VNC-nahe Funktionen prüfen, dazu neue oder veränderte Benutzerkonten, geänderte Systemkonfiguration und unerwartete ausgehende Verbindungen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Cloud- und PaaS-Instanzen gesondert klären

Für gehostete Instanzen den Patch-Stand schriftlich mit Fortinet bzw. Ihrem Betreiber abstimmen und das Ergebnis dokumentieren – bei aktiv ausgenutzten Schwachstellen gehört dieser Nachweis in die Vorfalls- und Compliance-Akte.

Kompromittierungs-Indikatoren (IoCs)

WO SUCHEN

Zugriffs-Logs der Web-Oberfläche HTTPS/443 – Anfragen an VNC-nahe Funktionen

AUFFÄLLIGE MUSTER

Shell-Sonderzeichen in HTTP-Parametern `|` `;` `&` `$(` `)` `` ` `` · Anfragen ohne vorherige Anmeldung

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; belastbare Indikatoren aus der beobachteten Aktivität liegen öffentlich nicht vor. Die genannten Muster sind Suchhinweise für Ihre eigene Log-Auswertung – kein abschließender Nachweis und kein Ersatz für eine forensische Prüfung bei konkretem Verdacht.

Wichtig: FortiSandbox verarbeitet genau die Dateien, die Sie für verdächtig halten. Wer das System übernimmt, sieht Ihre Analyse-Ergebnisse, kann Bewertungen manipulieren und steht in einem Segment, dem Ihre übrigen Systeme vertrauen. Ohne Auswertung der Zugriffs-Logs bleibt ein bereits erfolgter Zugriff 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: Unauthentifizierte Anfragen an die Sandbox-Oberfläche 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 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 der Management-Oberfläche heute einschränken, Patch kurzfristig einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Patch-Stand der Cloud-/PaaS-Instanzen schriftlich beim Hersteller bestätigen lassen.

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-2026-25089 und dem FortiSandbox-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-26-141 · NVD CVE-2026-25089 · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 16.07.2026) · Berichte zu beobachteten Angriffsversuchen (Defused, KEVIntel). 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.