THREAT INTELLIGENCE BRIEFING

CVE-2026-126259

Befehlsausführung als Super-Admin über HA-Pakete in FortiOS.

FortiOS prüft bei bestimmten Hochverfügbarkeits-Paketen nicht, ob die Gegenstelle berechtigt ist. Ist eine FortiGate mit FGSP und standalone-config-sync oder mit Autoscale konfiguriert, kann ein Angreifer ohne Anmeldung über präparierte HA-Pakete Befehle als Super-Admin ausführen. Fortinet hat die Lücke am 10.11.2026 mit 8.0.1, 7.6.8, 7.4.13 und 7.2.14 geschlossen; eine Ausnutzung ist bislang nicht bekannt.

> **Geschäftsrisiko:** Vollständige Übernahme der Firewall mit Super-Admin-Rechten – mit Zugriff auf Regeln, VPN-Zugänge und Zugangsdaten, Einstieg 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 9,0. Angreifbar sind nur Geräte mit HA FGSP plus standalone-config-sync oder mit Autoscale.

AUSNUTZUNG
Nicht bekannt (Stand 11.11.2026)

BETROFFEN
FortiOS 8.0.0, 7.6.0–7.6.7, 7.4.0–7.4.12 7.2.0–7.2.13, 7.0 (alle) · nur mit FGSP + standalone-config-sync oder Autoscale

HANDLUNGSBEDARF
Dringend – vor Ausnutzungsbeginn patchen

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Ohne Anmeldung
FGSP-Config-Sync / Autoscale · CWE-306

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

8.0.1 · 7.6.8 · 7.4.13 · 7.2.14
Fixversionen seit 10.11.2026

Die Ursache: Mit **FGSP** (FortiGate Session Life Support Protocol) und der Option **standalone-config-sync** bzw. mit **Autoscale** tauschen FortiGates Sitzungs- und Konfigurationsdaten über HA-Pakete aus. Laut Fortinet fehlt dabei für eine kritische Funktion die Authentifizierung (**CWE-306, Missing Authentication for Critical Function**). Ein nicht authentifizierter Angreifer kann so mit präparierten HA-Paketen Befehle mit **Super-Admin-Rechten** ausführen. Geräte ohne diese Konfiguration nennt Fortinet nicht als angreifbar. Fortinet hat die Lücke intern gefunden und nennt keine weiteren technischen Details.

ANGRIFFSKETTE

01 **Konfiguration aktiv** – FortiGate nutzt FGSP mit standalone-config-sync oder Autoscale

02 **Präparierte HA-Pakete** – Angreifer sendet Synchronisationspakete ohne Anmeldung

03 **Keine Prüfung** – die kritische Funktion verlangt keine Authentifizierung

04 **Super-Admin** – Befehle mit vollen Rechten auf der Firewall

Betroffenheit & Fixversionen

Produkt · Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 8.0	8.0.0	8.0.1
FortiOS 7.6	7.6.0 bis 7.6.7	7.6.8
FortiOS 7.4	7.4.0 bis 7.4.12	7.4.13
FortiOS 7.2	7.2.0 bis 7.2.13	7.2.14
FortiOS 7.0	Alle Versionen	Migration auf einen korrigierten Zweig

Angaben laut Fortinet-Advisory FG-IR-26-273. Betroffen sind nur FortiGates mit **HA FGSP plus standalone-config-sync oder mit Autoscale**. Fortinet nennt **keinen Workaround**, aber einen virtuellen Patch (FG-VD-61445.0day, FMWP-DB-Update 26.082). Für 7.0 gibt es keinen Fix im Zweig. Ältere Zweige führt das Advisory nicht auf.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff auf die Firewall 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

10.11.2026
FG-IR-26-273 · Fix 8.0.1 / 7.6.8 / 7.4.13 / 7.2.14

10.11.2026
Fortinet: keine Ausnutzung bekannt · virtueller Patch

11.11.2026
NVD veröffentlicht CVE-2026-126259

Stand heute
Nicht in CISA KEV · kein PoC

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
FGSP/Autoscale prüfen	Update einspielen	Logs prüfen

01 Betroffenheit feststellen

Version aller FortiGates prüfen: `8.0.0`, `7.6.0`–`7.6.7`, `7.4.0`–`7.4.12`, `7.2.0`–`7.2.13` und alle `7.0`-Versionen sind betroffen. Angreifbar sind laut Fortinet nur Geräte mit HA FGSP plus standalone-config-sync oder mit Autoscale – diese Konfiguration je Gerät klären.

02 Patchen

Auf `8.0.1`, `7.6.8`, `7.4.13` bzw. `7.2.14` oder neuer aktualisieren; 7.0 auf einen korrigierten Zweig migrieren. Vorher ein Konfigurations-Backup sichern und den Upgrade-Pfad im Fortinet-Upgrade-Tool prüfen.

03 Risiko bis zum Update senken

Fortinet nennt keinen Workaround, stellt aber den virtuellen Patch `FG-VD-61445.0day` im FMWP-DB-Update `26.082` bereit. Zusätzlich sicherstellen, dass die Schnittstellen für die HA-Synchronisation nur zwischen den Cluster-Mitgliedern erreichbar sind.

04 Kompromittierung ausschließen

Event-Logs auf unerwartete Konfigurationsänderungen, neue Admin-Konten und ungewöhnliche Synchronisationsvorgänge prüfen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

Kompromittierungs-Indikatoren (IoCs)

ÖFFENTLICHE IOCS

Keine – Fortinet nennt keine, Ausnutzung nicht bekannt

AUSWERTUNGSQUELLEN

FortiGate-Event- und System-Logs
Logs der HA-/Sync-Schnittstellen

AUFFÄLLIGE MUSTER

HA-Pakete von Adressen außerhalb des Clusters
unerwartete Konfigurationsänderungen oder Admin-Konten

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

Wichtig: Betroffen sind nur FortiGates mit FGSP plus standalone-config-sync oder mit Autoscale – dort aber mit vollen Super-Admin-Rechten und ohne Anmeldung.

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: Ein HA-Synchronisationspaket von außerhalb des Clusters fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden FortiGates mit FGSP-Config-Sync oder Autoscale 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 FortiOS-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 FortiGates mit FGSP-Config-Sync oder Autoscale auf die Fixversionen anordnen.
- Bestätigen lassen, welche Geräte diese Konfiguration nutzen und dass 7.0 migriert wird.
- Über eine dauerhafte Überwachung der Firewall-Infrastruktur 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-2026-126259 und dem FortiOS-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: Fortinet PSIRT FG-IR-26-273 (10.11.2026, Fixversionen, CVSS 9,0, virtueller Patch) · NVD (CVSS 3.1 Basiswert 9,8) · CISA KEV (Stand 11.11.2026: nicht gelistet). Stand 11.11.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.