AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-25249

Heap-Overflow im CAPWAP-Dienst: FortiGate ohne Anmeldung übernehmbar.

Der CAPWAP-Dienst, über den FortiGate-Firewalls ihre Access Points und Switches steuern, enthält einen Heap-Overflow: Wer ihn über UDP-Port 5246 erreicht, kann ohne Anmeldung eigenen Code auf der Firewall ausführen. Fortinet hat die Lücke im Januar 2026 geschlossen. Seit dem Sommer wird sie aktiv ausgenutzt, um den Node.js-Trojaner PivotC2 zu installieren, der Konfiguration und Zugangsdaten entschlüsselt und die Firewall zum Sprungbrett ins interne Netz macht. Seit dem 9. September 2026 steht die Schwachstelle im CISA-Katalog aktiv ausgenutzter Schwachstellen – mit forensischer Triage-Pflicht.

Geschäftsrisiko: vollständige Übernahme der Firewall mit Zugriff auf VPN-Schlüssel, Admin-Konten und WLAN-Passwörter – als Ausgangspunkt für Lateral Movement, Postfach-Abfluss und Erpressung; ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO ist in diesem Fall wahrscheinlich.

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 eines Nutzers, mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. Der Basiswert 9,8 ist die NVD-Bewertung. Fortinet selbst stuft die Schwachstelle als CNA mit 8,1 (AC:H) bzw. inklusive Temporal-Metriken mit 7,4 ein – die Angriffskomplexität wird dort höher gewichtet. Die dokumentierte Ausnutzung in der Praxis spricht für die NVD-Lesart.

AUSGENUTZT SEIT
spätestens Juli 2026

BETROFFEN
FortiOS 6.4 – 7.6.3
FortiSwitchManager 7.0/7.2 · FortiSASE

HANDLUNGSBEDARF
Sofort

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Basiswert (NVD)

Heap-Overflow
cw_acd · CAPWAP · UDP 5246

Aktiv
ausgenutzt · CISA KEV · Frist 12.09.2026

Ohne CAPWAP
auf exponierten Interfaces nicht erreichbar

Die Ursache: Der Daemon `cw_acd` (CAPWAP Wireless Aggregate Controller) verarbeitet auf FortiGate und FortiSwitchManager die Steuerkommunikation mit FortiAPs und FortiSwitches. Beim Parsen speziell präparierter CAPWAP-Pakete schreibt er über das Ende eines Heap-Puffers hinaus (**CWE-122**). Ein Angreifer, der den Dienst erreicht, kann damit den Programmfluss übernehmen und Befehle mit den Rechten des Daemons ausführen – **ohne Zugangsdaten, ohne Nutzerinteraktion**. Erreichbar ist der Dienst überall dort, wo ein Interface CAPWAP bzw. „Fabric"-Zugriff erlaubt – auf falsch konfigurierten WAN-Ports also direkt aus dem Internet. Fortinet fand die Lücke intern; die beobachteten Angreifer nutzen laut SOCRadar CAPWAP-Discovery-Antworten, um die Adressverwürfelung (ASLR) auszuhebeln.

ANGRIFFSKETTE

01	02	03	04
Dienst exponiert – CAPWAP (UDP 5246) auf einem aus dem Internet erreichbaren Interface	**Präpariertes Paket** – Heap-Overflow in cw_acd, ASLR über Discovery-Antworten umgangen	**Codeausführung** – Node.js-Reverse-Shell auf der Firewall, PivotC2 wird nachgeladen	**Ausbreitung** – Konfiguration entschlüsselt, VPN-/Admin-Zugänge gestohlen, Tunnel ins LAN

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.6	`7.6.0 – 7.6.3`	`7.6.4 oder höher`
FortiOS 7.4	`7.4.0 – 7.4.8`	`7.4.9 oder höher`
FortiOS 7.2	`7.2.0 – 7.2.11`	`7.2.12 oder höher`
FortiOS 7.0	`7.0.0 – 7.0.17`	`7.0.18 oder höher`
FortiOS 6.4	alle Versionen	Migration auf gefixten Zweig
FortiSwitchManager 7.2	`7.2.0 – 7.2.6`	`7.2.7 oder höher`
FortiSwitchManager 7.0	`7.0.0 – 7.0.5`	`7.0.6 oder höher`
FortiSASE 25.1 / 25.2	`25.1.a.2 · 25.2.b`	durch Fortinet behoben (25.1.b / 25.2.c)

Für den Zweig 6.4 nennt Fortinet als CNA **keinen** eigenen Fix (Drittquellen führen 6.4.17 an) – hier ist der Wechsel auf einen unterstützten Zweig der belastbare Weg. FortiSASE wurde cloudseitig von Fortinet gepatcht, Kunden müssen dort nichts tun. Siemens RUGGEDCOM APE1808 mit Fortinet-NGFW ist ebenfalls betroffen (SSA-864900). Exakte Build-Stände gegen FG-IR-25-084 abgleichen.

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

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

01 Betroffenheit feststellen

Firmware-Stand aller FortiGates und FortiSwitchManager-Instanzen erheben (betroffen: alles unterhalb 7.6.4 / 7.4.9 / 7.2.12 / 7.0.18 sowie ganz 6.4). Dann prüfen, auf welchen Interfaces CAPWAP bzw. `fabric` in den Zugriffsrechten steht – jedes WAN-Interface mit diesem Eintrag ist aus dem Internet angreifbar.

```
show system interface | grep -B3 -A3 allowaccess
```

02 Sofort mitigieren (vor dem Patch)

Auf exponierten Interfaces den `fabric`-Zugriff entfernen, sodass nur die benötigten Dienste bleiben. Alternativ CAPWAP per Local-in-Policy auf die IP-Adressen der eigenen Access Points und Switches beschränken (Service UDP 5246-5249, alles andere verwerfen). Beides ist von Fortinet als Workaround dokumentiert.

```
config system interface · edit "wan1" · set allowaccess ping https ssh · next · end
```

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren: `7.6.4` · `7.4.9` · `7.2.12` · `7.0.18` (FortiOS) bzw. `7.2.7` · `7.0.6` (FortiSwitchManager). Für 6.4 gibt es keinen Fix im eigenen Zweig – Migration einplanen. Vorher Konfigurationssicherung ziehen; HA-Cluster nach Fortinet-Upgrade-Pfad aktualisieren.

04 Kompromittierung ausschließen

Der Patch schließt die Tür – er wirft niemanden hinaus, der schon drin ist. Auf jeder Firewall, deren CAPWAP-Dienst erreichbar war, nach Node.js-Prozessen und der Datei `/tmp/.i.js` suchen, ausgehende TLS-Verbindungen der Firewall selbst zu unbekannten Zielen prüfen und die IoCs unten abgleichen. CISA verlangt für Bundesbehörden hier ausdrücklich eine forensische Triage – das ist auch für Sie der richtige Maßstab.

05 Bei Verdacht: Zugangsdaten als offengelegt behandeln

PivotC2 entschlüsselt die Gerätekonfiguration inklusive VPN-Pre-Shared-Keys, SSL-VPN-Zugängen, WLAN-Passwörtern und Admin-Konten. Bei jedem Hinweis auf einen Zugriff: sämtliche lokal gespeicherten Geheimnisse erneuern, Zertifikate tauschen, Regelwerk auf fremde Einträge prüfen – und die Beweise für eine etwaige Meldung sichern, bevor das Gerät neu aufgesetzt wird.

Kompromittierungs-Indikatoren (IoCs)

DATEIARTEFAKTE AUF DER FIREWALL

`/tmp/.i.js` (PivotC2, Node.js)
Exploit-Dropper `fortirun.bin`

NETZWERK

Eingehend: CAPWAP UDP 5246 aus fremden Quellen
Ausgehend: TLS-Verbindungen der Firewall selbst, SOCKS5-/HTTP-Tunnel, Exfiltration in Wasabi-Cloud-Speicher

VERHALTEN

Unerwartete Node.js-Prozesse auf FortiGate,
Anmeldungen mit aus der Konfiguration stammenden VPN-/Admin-Zugängen aus neuen Quellen

Zur Einordnung: Die Indikatoren stammen aus der Kampagnenanalyse der SOCRadar Threat Research Unit und sind von Fortinet nicht als offizielle IoCs bestätigt; Dateinamen und Infrastruktur sind trivial änderbar. Belastbarer als die Suche nach einem Dateinamen ist die Frage, ob der CAPWAP-Dienst des Geräts seit Januar 2026 aus dem Internet erreichbar war.

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: Ausgehende Verbindungen der Firewall zu unbekannten Zielen und die Wiederverwendung ihrer VPN-Zugangsdaten aus fremden Quellen 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 CAPWAP-Dienste auf FortiGate-Firewalls 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

- Heute anordnen: CAPWAP auf allen extern erreichbaren Interfaces sperren, Patch innerhalb der Woche.
- Für jede FortiGate mit exponiertem CAPWAP-Dienst eine forensische Prüfung beauftragen – dokumentiert für eine etwaige Meldung.
- Geräte auf FortiOS 6.4 als Migrationsprojekt aufsetzen – dort gibt es keinen Fix mehr.

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-2025-25249 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 Advisory FG-IR-25-084 · CVE-Record CVE-2025-25249 (Fortinet als CNA) · NVD CVE-2025-25249 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 09.09.2026) · Siemens ProductCERT SSA-864900 · SOCRadar Threat Research Unit, Analyse der PivotC2-Kampagne (September 2026). Angaben nach bestem Wissen zum Stand 14.09.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.