AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-55591

Authentifizierungs-Bypass zu Super-Admin in Fortinet FortiOS & FortiProxy.

Ein nicht authentifizierter Angreifer aus dem Internet kann über gezielte Anfragen an das Node.js-Websocket-Modul die Authentifizierung umgehen und sich Super-Admin-Rechte auf der Appliance verschaffen – bis hin zum Anlegen eigener Administrator-Konten und dem Aufbau von SSL-VPN-Tunneln. Die Ausnutzung ist trivial und läuft nachweislich seit Mitte November 2024.

> **Geschäftsrisiko:** vollständige Übernahme der Firewall bzw. des Proxys – mit Potenzial zum Abschalten von Schutzregeln, Datenabfluss, Weiterbewegung ins interne Netz 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 Rechte, ohne Zutun – mit voller Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD weist den Basiswert 9,8 aus; Fortinet nennt mit Temporal-Metriken 9,6.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
16. November 2024	FortiOS 7.0.0 – 7.0.16 FortiProxy 7.0 & 7.2 (Management aus dem Netz erreichbar)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Super-Admin
Auth-Bypass via Node.js-Websocket

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

7.2/7.4/7.6
FortiOS ab 7.2 nicht betroffen

Die Ursache: Das Node.js-Websocket-Modul des Verwaltungsdienstes prüft die Herkunft eingehender Anfragen unzureichend. Über gezielt gestaltete Anfragen an dieses alternative Kommunikations-Channel (CWE-288) lässt sich die reguläre Authentifizierung vollständig umgehen. In Verbindung mit CSF-Proxy-Anfragen wird die Session so verarbeitet, als bestünde bereits eine gültige Super-Admin-Autorisierung – der Angreifer erhält administrative Kontrolle über `jsconsole`.

ANGRIFFSKETTE

01	02	03	04
Management exponiert – die administrative HTTP/HTTPS-Oberfläche ist aus dem Internet erreichbar	**Websocket ansprechen** – gestaltete Anfrage an das interne Node.js-Websocket-Modul	**Auth umgehen** – die Session wird als Super-Admin über `jsconsole` autorisiert	**Übernahme** – neue Admin-/lokale Konten anlegen, Policies ändern, SSL-VPN-Tunnel aufbauen

Betroffenheit & Fixversionen

Produkt / Zweig	Verwundbar bis	Fixversion (Ziel)
FortiOS 7.0	`7.0.0 – 7.0.16`	`7.0.17`
FortiProxy 7.0	`7.0.0 – 7.0.19`	`7.0.20`
FortiProxy 7.2	`7.2.0 – 7.2.12`	`7.2.13`
FortiOS 7.2 · 7.4 · 7.6	nicht betroffen	—
FortiProxy 7.4 · 7.6	nicht betroffen	—

Betroffen sind ausschließlich FortiOS 7.0.0 – 7.0.16 sowie FortiProxy 7.0.0 – 7.0.19 und 7.2.0 – 7.2.12 mit erreichbarem Management. FortiOS ab 7.2 sowie FortiProxy 7.4/7.6 sind laut Fortinet nicht angreifbar. Exakte Build-Stände gegen das Hersteller-Advisory FG-IR-24-535 des eigenen Zweigs abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Super-Admin-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

16.11.2024
Erste jsconsole-Ausnutzung in der Breite beobachtet (Arctic Wolf „Console Chaos“)

04.12.2024
Angreifer setzen SSL-VPN-Konfigurationen und neue Admin-Konten

14.01.2025
Fortinet veröffentlicht Advisory FG-IR-24-535 · CISA nimmt CVE in KEV auf

21.01.2025
CISA-Frist zum Handeln für Bundesbehörden (BOD 22-01)

Ihr Maßnahmenplan.

In dieser Reihenfolge – Perimeter schließen vor Patch, Patch vor Entwarnung.

01 Exposition sofort beenden

Prüfen, ob die administrative HTTP/HTTPS-Oberfläche aus dem Internet erreichbar ist. Als Sofortmaßnahme das HTTP/HTTPS-Management auf internetseitigen Schnittstellen deaktivieren oder per Local-in-Policy auf vertrauenswürdige Quell-Adressen beschränken. Bei Bedarf CSF (Security Fabric) per CLI abschalten.

02 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren: `FortiOS 7.0.17` · `FortiProxy 7.0.20` · `FortiProxy 7.2.13` (oder neuer). Der Fix schließt den Auth-Bypass über das Node.js-Websocket-Modul.

03 Kompromittierung ausschließen

Konfiguration und Audit-Logs auf unbekannte, seit Mitte November 2024 angelegte Administrator-/lokale Konten prüfen. Auf Login-Events mit `ui="jsconsole"` und `logdesc="Admin login successful"` aus unerwarteten Quellen achten sowie auf `cfgpath="system.admin" action="Add"`. Bekannte Angreifer-Kontennamen und Quell-IPs unten abgleichen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

04 Kompromittierte Appliance bereinigen

Bei Fund unbekannter Admin-Konten: Konten entfernen, Zugangsdaten und Zertifikate rotieren, SSL-VPN- und Policy-Konfiguration auf manipulierte Änderungen prüfen. Im Zweifel Neuaufsetzen aus einem sauberen Stand erwägen und Incident Response einbinden.

05 Dauerhaft absichern

Management-Interfaces grundsätzlich nicht ins Internet exponieren, sondern über VPN/Jump-Host erreichbar machen. Herstellerseitige Updates zeitnah einspielen und die Auth-Logs des Perimeters kontinuierlich auswerten.

Kompromittierungs-Indikatoren (IoCs)

LOG-MARKER

```
logdesc="Admin login
successful" ui="jsconsole"
logdesc="Object attribute
configured"
cfgpath="system.admin"
action="Add"
```

NEU ANGELEGTE KONTEN

Zufällige Namen wie `Gujhmk`, `Ed8x4k`, `G0xgey`, `watchTowr`, `fortinet-support`

ANGREIFER-QUELL-IPS

`45.55.158.47` (häufigste) · `87.249.138.47` `155.133.4.175` · `37.19.196.65` `149.22.94.37` · `158.255.215.126`

Zur Einordnung: Die genutzten Kontennamen und Quell-IPs sind eine Momentaufnahme der beobachteten Kampagne und flüchtig – kein Ersatz für eine vollständige Prüfung aller Administrator-Konten und Audit-Logs. Der Erfolg zeigt sich vor allem an neuen, nicht autorisierten Admin-Konten und jsconsole-Logins seit Mitte November 2024.

Wichtig: Erfolgreiche Angriffe erscheinen als reguläre Admin-Logins über die jsconsole an gültigen Diensten – ohne Alarm. Ohne Prüfung der Konten- und Audit-Logs bleibt ein bereits erfolgter Zugriff unsichtbar, selbst nach dem Patch.

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: Die Anlage eines neuen Admin-Kontos und jsconsole-Admin-Logins 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 internetseitig exponierte, ungepatchte FortiOS-/FortiProxy-Management-Interfaces 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

- Management-Zugang heute vom Internet trennen, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein unbefugtes Admin-Konto angelegt wurde – dokumentiert für eine etwaige Meldung.
- Über eine dauerhafte Überwachung des Perimeters und der Management-Interfaces 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-2024-55591 und dem FortiOS-Perimeter.

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

Termin buchen

Quellen: Fortinet PSIRT Advisory FG-IR-24-535 · NIST NVD CVE-2024-55591 · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 14.01.2025, Frist 21.01.2025) · Arctic Wolf Labs „Console Chaos“ Threat Report. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Zweigs abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.