AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-40766

Improper Access Control in SonicWall SonicOS.

Ein nicht authentifizierter Angreifer aus dem Internet kann über eine fehlerhafte Zugriffskontrolle in der SonicOS-Verwaltung auf geschützte Ressourcen zugreifen und die Firewall unter bestimmten Bedingungen zum Absturz bringen. Betroffen sind die Management-Schnittstelle und der SSLVPN-Dienst der Gerätegenerationen 5, 6 und 7. Die Lücke wird seit Ende 2024 aktiv durch Ransomware-Gruppen – insbesondere Akira und Fog – über SSLVPN-Zugänge ausgenutzt.

> **Geschäftsrisiko:** unbefugter Fernzugriff auf das Firmennetz über kompromittierte SSLVPN-Konten und Ausfall der Firewall – mit Potenzial für Ransomware-Verschlüsselung, Datenabfluss, Betriebsunterbrechung und einen 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 – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. NVD-Basiswert 9,8 (CVSS 3.1); SonicWall selbst bewertet die Lücke mit 9,3 (Vektor mit veränderter Wirkungsdomäne). Eine CVSS-4.0-Bewertung liegt beim NVD nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
September 2024	SonicOS Gen 5, Gen 6 & Gen 7 (Management-Zugriff & SSLVPN)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Access-Control
Management-Zugriff & SSLVPN

Aktiv
ausgenutzt · CISA KEV · Ransomware

Akira / Fog
über SSLVPN-Konten

Die Ursache: SonicOS setzt in den betroffenen Versionen die Zugriffskontrolle in der Management-Ebene fehlerhaft durch. Ein nicht authentifizierter Angreifer kann dadurch auf eigentlich geschützte Ressourcen zugreifen; in bestimmten Konfigurationen führt der Zugriff zusätzlich zu einem Absturz der Firewall. Ransomware-Akteure nutzen die Schwäche vor allem, um sich über den SSLVPN-Dienst mit lokalen Benutzerkonten Zugang zum internen Netz zu verschaffen.

ANGRIFFSKETTE

01 **Gerät exponiert** – SonicOS-Management bzw. SSLVPN-Portal ist aus dem Internet erreichbar

02 **Zugriffskontrolle umgehen** – fehlerhafte Access-Control-Prüfung erlaubt Zugriff ohne gültige Authentifizierung

03 **SSLVPN-Konto übernehmen** – lokale Benutzerkonten (oft mit schwachen/geerbten Passwörtern) werden für den VPN-Zugang missbraucht

04 **Netz-Zugang** – Angreifer bewegt sich ins interne Netz; Akira/Fog leiten Ransomware-Angriff ein

Betroffenheit & Fixversionen

SonicOS-Generation	Verwundbar bis	Fixversion (Ziel)
Gen 5 (SOHO)	≤ 5.9.2.14-12o	5.9.2.14-13o
Gen 6 (SM9800 · NSsp 12400/12800)	≤ 6.5.4.14-109n	6.5.2.8-2n
Gen 6 (übrige Appliances)	≤ 6.5.4.14-109n	6.5.4.15-116n
Gen 7	≤ 7.0.1-5035	7.0.1-5036 / 7.3.0

Die betroffenen Versionen (Gen 5 ≤ 5.9.2.14-12o, Gen 6 ≤ 6.5.4.14-109n, Gen 7 ≤ 7.0.1-5035) sind durch NVD bestätigt. Die genannten Fix-Builds stammen aus SonicWall-Advisory-Angaben, konnten hier aber nicht direkt aus dem PSIRT-Portal verifiziert werden – exakte Zielversion je Modell und Build zwingend gegen **SNWLID-2024-0015** für das eigene Gerät abgleichen. Für Gen 7 empfiehlt SonicWall in späteren Hinweisen SonicOS 7.3.0.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff oder eine Ransomware-Kompromittierung 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

22.08.2024
SonicWall veröffentlicht Advisory SNWLID-2024-0015

09.09.2024
Aufnahme in CISA KEV · als Ransomware-genutzt markiert

Ab Sep 2024
Akira/Fog nutzen SSLVPN-Zugänge aktiv aus (Arctic Wolf)

Jul–Aug 2025
Erneute Angriffswelle gegen Gen-7-Firewalls

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
SSLVPN/Management absichern	Firmware patchen	Passwörter zurücksetzen · Threat Hunting

01 Betroffenheit feststellen

SonicOS-Generation und Build ermitteln und gegen die betroffenen Versionen prüfen (Gen 5 ≤ 5.9.2.14-12o, Gen 6 ≤ 6.5.4.14-109n, Gen 7 ≤ 7.0.1-5035). Prüfen, ob Management-Interface oder SSLVPN aus dem Internet erreichbar sind.

02 Sofort absichern (vor dem Patch)

Management-Zugriff und SSLVPN aus dem Internet einschränken – Zugang auf vertrauenswürdige Quell-IPs begrenzen bzw. SSLVPN deaktivieren, wo nicht zwingend benötigt. Multi-Faktor-Authentisierung für alle VPN-Konten erzwingen.

03 Patchen

Auf die Fixversion der eigenen Generation aktualisieren (`5.9.2.14-13o · 6.5.4.15-116n bzw. 6.5.2.8-2n · 7.0.1-5036 / 7.3.0`). Exakte Zielversion je Modell gegen das Hersteller-Advisory SNWLID-2024-0015 abgleichen.

04 Lokale Passwörter zurücksetzen

SonicWall weist ausdrücklich darauf hin: Passwörter aller lokalen Benutzerkonten mit SSLVPN-Berechtigung zurücksetzen – besonders von Gen 6 nach Gen 7 migrierte Konten. Der Patch allein schließt geerbte/geleakte Zugangsdaten nicht.

05 Kompromittierung ausschließen

SSLVPN- und Admin-Anmeldungen auf ungewöhnliche Quell-IPs, unbekannte Konten und untypische Zeiten durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff. Bei Verdacht Incident Response auslösen.

Kompromittierungs-Indikatoren (IoCs)

ANGRIFFSVEKTOR	AUFFÄLLIGE MARKER	RANSOMWARE-BEZUG
`SSLVPN-Anmeldungen` `SonicOS-Management-Zugriff`	SSLVPN-Logins lokaler Konten aus untypischen Quell-IPs · gehäufte Fehlversuche · von Gen 6 migrierte Konten	`Akira` · `Fog` nachgelagerte Verschlüsselung im Netz

Zur Einordnung: Für diese Schwachstelle sind keine stabilen technischen IoCs (feste IPs/Hashes) veröffentlicht – die Ausnutzung erfolgt über legitime SSLVPN-Anmeldungen mit gültigen Konten. Entscheidend ist die Auswertung der VPN-/Auth-Logs auf anomale Anmeldemuster; die genannten Marker sind eine Momentaufnahme der beobachteten Kampagnen.

Wichtig: Erfolgreiche Zugriffe erscheinen als reguläre SSLVPN-Anmeldungen gültiger lokaler Konten – ohne Alarm. Wer nur patcht, aber lokale Passwörter nicht zurücksetzt und den Perimeter nicht einschränkt, hat neuere Firmware bei unveränderter Angriffsfläche.

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: Anomale SSLVPN-Anmeldungen lokaler Konten und Management-Zugriffe 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, ungepatchte SonicWall-Firewalls mit aktivem SSLVPN 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 SonicOS-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

- Perimeter heute einschränken (SSLVPN/Management), Patch kurzfristig einspielen.
- Alle lokalen SSLVPN-Passwörter zurücksetzen und MFA erzwingen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.

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-2024-40766 und dem SonicOS-Perimeter.

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

Termin buchen

Quellen: NVD CVE-2024-40766 · SonicWall PSIRT Advisory SNWLID-2024-0015 · CISA Known Exploited Vulnerabilities Catalog (Ransomware-genutzt) · Arctic Wolf / Berichte zu Akira- und Fog-Ransomware. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges je Modell gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.