AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2024-53704

Authentifizierungs-Bypass im SonicWall SSL-VPN.

Ein nicht authentifizierter Angreifer aus dem Internet kann den Anmelde-Mechanismus des SSL-VPN umgehen und eine aktive VPN-Sitzung übernehmen – und erhält so Zugang ins interne Netz, während der legitime Nutzer abgemeldet wird. Voraussetzung ist ein aus dem Internet erreichbares SSL-VPN; die Ausnutzung ist trivial und läuft seit Februar 2025.

> **Geschäftsrisiko:** unbefugter Fernzugriff auf das interne Netz über gekaperte VPN-Sitzungen – mit Potenzial für 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/NIST wertet 9,8 (kritisch); SonicWall selbst stuft die Lücke im eigenen Advisory mit 8,2 (hoch) ein.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
18. Februar 2025	SonicOS 7.1.x & 8.0.0 Gen7-Firewalls · NSv · TZ80	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad (NVD)

Auth-Bypass
SSL-VPN Session-Hijacking

Aktiv
ausgenutzt · CISA KEV · PoC öffentlich

SSL-VPN
nur bei aktiviertem SSL-VPN

Die Ursache: Verwundbare SonicOS-Versionen prüfen die Sitzung des SSL-VPN unzureichend: Der Authentifizierungs-Mechanismus lässt sich mit einer präparierten Anfrage umgehen. Ein Angreifer benötigt weder Zugangsdaten noch eine bestehende Sitzung – er kann eine **aktive SSL-VPN-Sitzung kapern** bzw. die Anmeldung vollständig umgehen und übernimmt damit den Netzzugang des Opfers. Der legitime Nutzer wird dabei abgemeldet.

ANGRIFFSKETTE

01 **Portal exponiert** – das SSL-VPN der SonicWall-Firewall ist aus dem Internet erreichbar

02 **Anfrage präparieren** – manipulierte Anfrage an den SSL-VPN-Dienst

03 **Anmeldung umgehen** – Authentifizierung ausgehebelt, aktive Sitzung übernommen

04 **Zugang** – VPN-Zugriff ins interne Netz; der legitime Nutzer wird abgemeldet

Betroffenheit & Fixversionen

Plattform / Serie	Verwundbar bis	Fixversion (Ziel)
Gen7-Firewalls	7.1.1-7040 – 7.1.1-7058 · 7.1.2-7019	7.1.3-7015
Gen7 NSv	7.1.x (verwundbare Builds)	7.0.1-5165
TZ80	< 8.0.0-8037 (8.0.0-8035)	8.0.0-8037
Gen6 · Gen6.5	für diese CVE nicht gelistet	—

Betroffen sind Gen7-Hardware-Firewalls (NSa, NSsp, TZ-Serie), Gen7 NSv sowie der TZ80. Exploitierbar nur bei **aktiviertem SSL-VPN**. Exakte Build-Ranges des eigenen Modells gegen das SonicWall-Advisory SNWLID-2025-0003 abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff 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

05.11.2024
Computest Security meldet die Schwachstelle an SonicWall

07.01.2025
SonicWall veröffentlicht Advisory + Patches (noch keine Ausnutzung bekannt)

Mitte Feb. 2025
Bishop Fox veröffentlicht PoC-/Exploit-Details

18.02.2025
CISA KEV · aktive Ausnutzung in the wild bestätigt (Frist 11.03.2025)

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
SSL-VPN mitigieren / einschränken	Patch einspielen	Threat Hunting / Log-Analyse

01 Betroffenheit feststellen

Prüfen: Läuft eine der verwundbaren SonicOS-Versionen (7.1.1-7040 bis 7.1.1-7058, 7.1.2-7019, 8.0.0-8035) auf einer Gen7-Firewall, NSv oder einem TZ80? Ist das SSL-VPN aktiviert und aus dem Internet erreichbar? Nur diese Kombination ist angreifbar.

02 Sofort mitigieren (vor dem Patch)

Ist ein Patch nicht sofort möglich: SSL-VPN-Zugriff aus dem Internet deaktivieren oder auf vertrauenswürdige Quell-IPs beschränken. SonicWall benennt dies als Behelfsmaßnahme, bis der Patch eingespielt ist.

03 Patchen

Auf die Fixversion der eigenen Plattform aktualisieren (`Gen7 7.1.3-7015` · `NSv 7.0.1-5165` · `TZ80 8.0.0-8037` oder neuer). Danach das SSL-VPN wieder wie benötigt freigeben.

04 Kompromittierung ausschließen

SSL-VPN- und Authentifizierungs-Logs auf unerwartete Sitzungsübernahmen, plötzliche Abmeldungen legitimer Nutzer und Anmeldungen aus fremden Quellen durchsuchen. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Konten & Sitzungen härten

Aktive SSL-VPN-Sitzungen zurücksetzen, Zugangsdaten exponierter Konten rotieren und – falls noch nicht vorhanden – Multi-Faktor-Authentifizierung für den VPN-Zugang erzwingen, um den Missbrauch gekaperter Sitzungen zu erschweren.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE EREIGNISSE

unerwartete `SSL-VPN-Sitzungsübernahmen`
plötzliche Abmeldung legitimer Nutzer

LOG-QUELLEN

SonicOS `SSL-VPN- & Auth-Logs`
VPN-Sitzungs- und Login-Ereignisse

MARKER

VPN-Anmeldungen aus `unerwarteten Quell-IPs`
Sitzungen ohne vorausgehende Authentifizierung

Zur Einordnung: Für diese Schwachstelle liegen keine belastbaren, öffentlich bestätigten Netzwerk-IoCs (feste IPs/Hashes) vor. Erkennung erfolgt verhaltensbasiert über die Auswertung der SSL-VPN- und Authentifizierungs-Logs – kein Ersatz für eine gezielte Analyse Ihrer Umgebung.

Wichtig: Erfolgreiche Übernahmen erscheinen als scheinbar gültige SSL-VPN-Sitzungen. Ein deutliches Signal ist die unerwartete Abmeldung legitimer Nutzer. Ohne kontinuierliche Auswertung der VPN- und Auth-Logs bleibt ein bereits erfolgter Zugriff leicht 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: Anomale SSL-VPN-Sitzungsübernahmen und VPN-Anmeldungen aus unerwarteten Quellen fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte SSL-VPN-Portale von SonicWall-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 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

- SSL-VPN heute einschränken, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff über gekaperte VPN-Sitzungen erfolgt ist – dokumentiert für eine etwaige Meldung.
- Multi-Faktor-Authentifizierung und dauerhafte Überwachung des VPN-Perimeters 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-2024-53704 und dem SonicOS-Perimeter.

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

Termin buchen

Quellen: SonicWall PSIRT Advisory SNWLID-2025-0003 (CVE-2024-53704) · NIST NVD CVE-2024-53704 · CISA Known Exploited Vulnerabilities Catalog (hinzugefügt 18.02.2025) · Bishop Fox Exploit-Analyse. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen und Build-Ranges gegen das Hersteller-Advisory des jeweiligen Modells abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.