AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-40602

Rechteausweitung bis root in SonicWall SMA1000 (AMC).

Eine unzureichende Autorisierungsprüfung in der Management-Konsole (AMC) der SonicWall-SMA1000-Appliances erlaubt einem angemeldeten Nutzer, seine Rechte bis auf Root-Ebene auszuweiten. Als Zero-Day wurde die Lücke seit Dezember 2025 aktiv ausgenutzt – in Verkettung mit der kritischen Pre-Auth-Schwachstelle CVE-2025-23006 bis zur unauthentifizierten Codeausführung mit Root-Rechten. SonicWall-Firewalls und deren SSL-VPN sind nicht betroffen.

> **Geschäftsrisiko:** vollständige Übernahme des VPN-Zugangs-Gateways – mit Potenzial für Datenabfluss, dauerhaften Fernzugriff, Lateral Movement ins interne Netz und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

6,6 / 10

MITTEL
CVSS 3.1 BASISWERT

Niedrig | **Mittel** | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H` – über das Netzwerk erreichbar, mit hohem Aufwand und bereits vorhandenen hohen Rechten, ohne Nutzer-Zutun – volle Wirkung auf Vertraulichkeit, Integrität und Verfügbarkeit. In Verkettung mit CVE-2025-23006 (Pre-Auth-RCE) entsteht ein unauthentifizierter Angriff bis root.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Dezember 2025 (als Zero-Day)	SMA1000 12.4.3 & 12.5.0 Modelle SMA6200/6210 · 7200/7210 · 8200v	Sofort

Das Wichtigste in 60 Sekunden.

6,6 · MITTEL	Rechteausweitung	Aktiv	Firewalls
CVSS-Schweregrad	SMA1000 AMC bis root	Zero-Day · CISA KEV	& SSL-VPN nicht betroffen

Die Ursache: Die Appliance-Management-Konsole der SMA1000 führt eine Aktion mit unnötig hohen Rechten aus (CWE-250) und prüft dabei die Berechtigung des aufrufenden Nutzers nicht vollständig (CWE-862). Ein bereits angemeldeter Nutzer mit eingeschränkten Rechten kann so administrative bzw. Root-Rechte auf der Appliance erlangen. Verkettet mit **CVE-2025-23006** – einer kritischen Pre-Auth-Deserialisierungslücke im AMC/CMC – erhält ein Angreifer den Erstzugriff ohne Anmeldung und hebt sich anschließend über diese Lücke auf Root-Ebene.

ANGRIFFSKETTE

01	02	03	04
AMC exponiert – die SMA1000-Management-Konsole ist erreichbar	**Erstzugriff** – Codeausführung über die Pre-Auth-Lücke CVE-2025-23006	**Rechte ausweiten** – fehlende Autorisierung im AMC (CVE-2025-40602) → root	**Kontrolle** – Root auf dem VPN-Gateway: Persistenz, Datenzugriff, Lateral Movement

Betroffenheit & Fixversionen

SMA1000-Zweig	Verwundbar bis	Fixversion (Ziel)
12.4.3	≤ 12.4.3-03093 (platform-hotfix)	12.4.3-03245 (platform-hotfix)
12.5.0	≤ 12.5.0-02002 (platform-hotfix)	12.5.0-02283 (platform-hotfix)
SMA 100-Serie	nicht betroffen	—
Firewalls · SSL-VPN	nicht betroffen	—

Betrifft die SMA1000-Appliances SMA6200 · SMA6210 · SMA7200 · SMA7210 · SMA8200v. SonicWall-Firewalls, deren SSL-VPN-Dienste und die SMA-100-Serie sind laut Hersteller **nicht** betroffen. Die genannten Fix-Builds sind noch nicht gegen das Hersteller-Advisory verifiziert – exakte Version des eigenen Zweigs unbedingt gegen SNWLID-2025-0019 abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Root-Zugriff auf das VPN-Gateway 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

17.12.2025	17.12.2025	24.12.2025	Seither
SonicWall veröffentlicht Fixes (SNWLID-2025-0019)	CISA nimmt CVE in den KEV-Katalog auf	CISA-KEV-Frist für Bundesbehörden	Als Zero-Day ausgenutzt, verkettet mit CVE-2025-23006

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL
AMC-Zugang einschränken	Patch einspielen	Threat Hunting / Log-Analyse

01 Betroffenheit feststellen

Prüfen, ob eine SMA1000-Appliance (SMA6200/6210, 7200/7210, 8200v) im Einsatz ist und welche Version/Build läuft. SMA-100-Serie und Firewalls sind nicht betroffen. Nur die SMA1000-Management-Konsole (AMC) ist angreifbar.

02 Exposition sofort begrenzen (vor dem Patch)

Zugriff auf die Appliance-Management-Konsole (AMC) auf VPN oder feste Administrator-IP-Adressen beschränken. SSL-VPN-Management-Interface (AMC) und SSH aus dem öffentlichen Internet deaktivieren – das entzieht der Angriffskette den Erstzugriff.

03 Patchen

Auf die Fixversion des eigenen Zweigs aktualisieren (`12.4.3-03245` bzw. `12.5.0-02283` platform-hotfix oder höher). Exakte Build-Angabe vor dem Einspielen gegen das Hersteller-Advisory SNWLID-2025-0019 abgleichen.

04 Kompromittierung ausschließen

AMC- und Authentifizierungs-Logs auf unerwartete administrative Aktionen, neue/erhöhte Konten und Zugriffe aus fremden Quellen durchsuchen. Wegen der Verkettung mit CVE-2025-23006 gezielt auf Anzeichen einer Pre-Auth-Codeausführung achten. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 CVE-2025-23006 mit abdecken

Sicherstellen, dass auch die verkettete kritische Pre-Auth-Lücke CVE-2025-23006 im AMC/CMC geschlossen ist. Erst beide Fixes zusammen brechen die beobachtete Angriffskette bis root.

Kompromittierungs-Indikatoren (IoCs)

ZU PRÜFENDE KOMPONENTE

`SMA1000 Appliance Management Console (AMC)`
administrative Aktionen & Rechteänderungen

VERKETTETE LÜCKE

`CVE-2025-23006` – Pre-Auth-Deserialisierung im AMC/CMC (Erstzugriff der Kette)

NETZ-EXPOSITION

öffentlich erreichbares AMC / SSL-VPN-Management
SSH aus dem Internet

Zur Einordnung: SonicWall hat für CVE-2025-40602 keine atomaren Indikatoren (IPs/Hashes) veröffentlicht. Maßgeblich ist die Analyse der AMC- und Authentifizierungs-Logs auf unerwartete privilegierte Aktionen sowie auf Spuren der verketteten Pre-Auth-Lücke CVE-2025-23006 – kein Ersatz für eine strukturierte Log-Auswertung.

Wichtig: Die Rechteausweitung selbst erfordert einen bestehenden Zugang – gefährlich wird sie in der Kette: über CVE-2025-23006 verschafft sich ein Angreifer ohne Anmeldung Zugriff und hebt sich dann bis root. Erfolgreiche Schritte erscheinen als reguläre AMC-Aktionen. Ohne Auswertung der Management-Logs bleibt ein bereits erfolgter Zugriff 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: Unerwartete administrative Aktionen im AMC und anomale Zugriffe auf die SMA1000 fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden exponierte, ungepatchte SMA1000-Management-Konsolen 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 SonicWall-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

- AMC-Exposition heute einschränken, Patch innerhalb von 72 Stunden einplanen.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Sicherstellen, dass die verkettete Lücke CVE-2025-23006 mit geschlossen ist.

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-2025-40602 und dem SonicWall-Perimeter.

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

Termin buchen

Quellen: SonicWall PSIRT Advisory SNWLID-2025-0019 · NVD CVE-2025-40602 (CVSS 6,6 / CISA-ADP) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 17.12.2025, Frist 24.12.2025) · Tenable, Arctic Wolf und Help Net Security Threat Advisories. Angaben nach bestem Wissen zum Stand 14.07.2026; die genannten Fix-Builds sind noch nicht gegen das Hersteller-Advisory verifiziert und vor dem Einspielen gegen SNWLID-2025-0019 des eigenen Zweigs abzugleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.