AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2025-23006

Pre-Auth-Deserialisierung (RCE) in SonicWall SMA1000.

Ein nicht authentifizierter Angreifer aus dem Internet kann über die Management-Konsolen (AMC/CMC) der SMA1000-Appliance nicht vertrauenswürdige Daten deserialisieren lassen und unter bestimmten Bedingungen beliebige Betriebssystem-Befehle ausführen – ohne gültige Anmeldedaten. Die Lücke wurde bereits vor der Veröffentlichung als Zero-Day ausgenutzt. Die SMA 100-Serie und Firewalls sind nicht betroffen.

> **Geschäftsrisiko:** vollständige Kompromittierung des SMA1000-Fernzugriffs-Gateways – mit Potenzial für Eindringen ins interne Netz, Diebstahl von Zugangsdaten, Datenabfluss, Persistenz 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). Eine CVSS-4.0-Bewertung liegt beim NVD nicht vor.

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
Januar 2025 (Zero-Day)	SMA1000 ≤ 12.4.3-02804 (Konsolen AMC / CMC)	Sofort

Das Wichtigste in 60 Sekunden.

9,8 · KRITISCH
CVSS-Schweregrad

Pre-Auth-RCE
Deserialisierung in AMC/CMC (CWE-502)

Aktiv
als Zero-Day ausgenutzt · CISA KEV

SMA 100
& Firewalls nicht betroffen

Die Ursache: Verwundbare SMA1000-Versionen nehmen in den Management-Konsolen – Appliance Management Console (AMC) und Central Management Console (CMC) – von außen zugeführte, nicht vertrauenswürdige Daten entgegen und **deserialisieren** sie ohne Authentifizierung (CWE-502: Deserialization of Untrusted Data). Unter bestimmten Bedingungen lässt sich daraus die Ausführung beliebiger Betriebssystem-Befehle durch einen unauthentifizierten Angreifer aus der Ferne erzeugen – ein klassischer Pre-Auth-RCE-Pfad über eine unsichere Deserialisierung.

ANGRIFFSKETTE

01	02	03	04
Konsole exponiert – die Management-Konsole (AMC/CMC) der SMA1000 ist aus dem Internet erreichbar	**Daten einschleusen** – manipuliertes, serialisiertes Objekt an den ungeschützten Endpunkt der Konsole senden	**Deserialisierung** – die Appliance verarbeitet die Daten ohne Auth-Prüfung (CWE-502)	**OS-Befehle** – unauthentifizierte Ausführung beliebiger Betriebssystem-Befehle auf der Appliance

Betroffenheit & Fixversionen

SMA1000-Komponente	Verwundbar bis	Fixversion (Ziel)
SMA1000 (AMC/CMC)	≤ `12.4.3-02804`	`12.4.3-02854`
SMA 100-Serie	nicht betroffen	—
Firewalls · SSL-VPN	nicht betroffen	—

Betroffen ist ausschließlich die SMA1000-Serie über ihre Management-Konsolen AMC und CMC in Version `12.4.3-02804` und früher. Die SMA 100-Serie sowie SonicWall-Firewalls sind laut Hersteller **nicht** betroffen. Fix ab `12.4.3-02854` (platform-hotfix); exakte Builds gegen SNWLID-2025-0002 abgleichen.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff bzw. eine Codeausführung auf dem Fernzugriffs-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

22.01.2025
SonicWall veröffentlicht Advisory SNWLID-2025-0002 + Fix 12.4.3-02854

22.01.2025
Hinweise auf aktive Ausnutzung als Zero-Day

24.01.2025
CISA nimmt in KEV auf · Frist 14.02.2025

Seither
Fortlaufende Ausnutzung; später mit CVE-2025-40602 zu Root-RCE verkettet

Ihr Maßnahmenplan.

In dieser Reihenfolge – Konsole abschotten vor Patch, Patch vor Entwarnung.

SOFORT	KURZFRISTIG	PARALLEL
Management-Konsolen vom Internet trennen	Patch einspielen	Threat Hunting / Log-Analyse

01 Betroffenheit feststellen

Handelt es sich um eine SMA1000-Appliance mit Version `12.4.3-02804` oder früher? Sind die Management-Konsolen AMC und/oder CMC aus dem Internet oder aus nicht vertrauenswürdigen Netzen erreichbar? Die SMA 100-Serie und Firewalls sind nicht betroffen.

02 Sofort mitigieren (vor dem Patch)

Herstellerbehelf: den Zugriff auf die Appliance Management Console (AMC) und die Central Management Console (CMC) auf vertrauenswürdige Quellen beschränken – Management-Konsolen niemals offen ins Internet stellen.

03 Patchen

Auf `12.4.3-02854` (platform-hotfix) oder höher aktualisieren. SonicWall hat den Fix am 22.01.2025 veröffentlicht; er behebt die Deserialisierungs-Schwachstelle.

04 Kompromittierung ausschließen

Konsolen- und System-Logs auf unerwartete Betriebssystem-Befehle, neue Prozesse/Konten und Zugriffe aus fremden Quellen prüfen. Da die Lücke als Zero-Day ausgenutzt wurde, auch **vor** dem Patch-Zeitpunkt rückwirkend auswerten. Ein Patch schließt die Lücke – nicht einen bereits erfolgten Zugriff.

05 Perimeter härten

Grundsatz durchsetzen: Management-Interfaces nie direkt exponieren. Zusätzlich die verkettbare Schwachstelle `CVE-2025-40602` (Root-RCE in Kombination) mitbewerten und patchen.

Kompromittierungs-Indikatoren (IoCs)

ZU ÜBERWACHENDE ZUGÄNGE

Zugriffe auf die Management-Konsolen `AMC` und `CMC` der SMA1000 aus nicht vertrauenswürdigen Quellen

VERDÄCHTIGES VERHALTEN

unerwartete Betriebssystem-Prozesse oder -Befehle im Kontext des Konsolen-Dienstes · anomale Deserialisierungs-/Fehlermeldungen

PRÜFHINWEIS

da als Zero-Day ausgenutzt: Logs auch `vor` dem Patch-Zeitpunkt rückwirkend auswerten

Zur Einordnung: SonicWall veröffentlicht zu dieser Schwachstelle keine spezifischen technischen Indikatoren (IP-Adressen/Hashes). Die genannten Punkte sind Detektions-Leitlinien und kein Ersatz für die Analyse Ihrer Konsolen- und Systemlogs.

Wichtig: Da die Lücke bereits als Zero-Day ausgenutzt wurde, kann ein Zugriff vor dem Patch erfolgt sein. Ein reiner Patch entfernt bereits erlangten Zugriff, untergeschobene Konten oder Persistenz nicht – ohne Prüfung des Systems bleibt eine erfolgte Kompromittierung 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: Zugriffe auf AMC/CMC aus fremden Quellen und unerwartete OS-Befehle im Konsolen-Kontext 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 (AMC/CMC) 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 SMA1000-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-Konsolen (AMC/CMC) heute vom Internet trennen, Patch umgehend – die CISA-Frist (14.02.2025) ist längst überschritten.
- Prüfen lassen, ob bereits ein Zugriff erfolgt ist – dokumentiert für eine etwaige Meldung.
- Grundsatz durchsetzen: Management-Interfaces nie direkt exponieren.

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-2025-23006 und dem SMA1000-Perimeter.

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

Termin buchen

Quellen: SonicWall PSIRT Advisory SNWLID-2025-0002 (CVE-2025-23006) · NVD (nvd.nist.gov, CVSS 3.1 Basiswert 9,8, CWE-502) · CISA Known Exploited Vulnerabilities Catalog (Aufnahme 24.01.2025, Frist 14.02.2025). Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversionen gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.