AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-15410

Post-Auth-Code-Injection in der SonicWall SMA1000 Management Console.

In der Appliance Management Console (AMC) der SonicWall SMA1000-Serie steckt eine Code-Injection-Schwachstelle: Ein aus dem Netz erreichbarer, als Administrator angemeldeter Angreifer kann unter bestimmten Bedingungen beliebige Betriebssystem-Befehle auf der Appliance ausführen. Die Lücke wird aktiv ausgenutzt – in beobachteten Angriffen in Kombination mit der kritischen SSRF-Schwachstelle CVE-2026-15409, über die sich Angreifer die nötige Zugriffs- bzw. Administratorposition erst verschaffen. Seit dem 14. Juli 2026 ist die Schwachstelle im CISA-KEV-Katalog gelistet.

Geschäftsrisiko: Vollständige Übernahme des VPN-/Zugangs-Gateways und damit des Einfallstors ins Unternehmensnetz – mit Potenzial für Ausspähen von Zugangsdaten, laterale Bewegung, Datenabfluss und Betriebsunterbrechung. Da die SMA1000 den Fernzugang absichert, ist ein erfolgreicher Angriff regelmäßig ein meldepflichtiger Sicherheitsvorfall nach NIS-2 / DSGVO.

7,2 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H` – aus dem Netz ausnutzbar, aber erst nach Anmeldung mit Administrator-Rechten (PR:H) – dann jedoch vollständige Ausführung beliebiger Betriebssystem-Befehle auf der Appliance. Der Hersteller stuft die Lücke als „High“ ein; ein offizieller Basiswert liegt bei NVD (Status „Received“) und im PSIRT-Advisory bislang nicht vor. Der genannte Wert ist eine konservative Argos-Einschätzung nach CVSS 3.1 und noch nicht bestätigt.

AUSGENUTZT SEIT
14. Juli 2026 (als Zero-Day vor Veröffentlichung)

BETROFFEN
SMA1000 12.4.3-03245 bis 12.4.3-03434

HANDLUNGSBEDARF
Sofort

Das Wichtigste in 60 Sekunden.

7,2 · HOCH
CVSS 3.1 (Argos-Einschätzung)

Post-Auth (Admin)
Ausführung als angemeldeter Administrator

Aktiv
ausgenutzt · CISA KEV (seit 14.07.2026)

CWE-94
Code Injection / OS-Command-Execution

Die Ursache: Die Appliance Management Console (AMC) der SMA1000 kontrolliert die Generierung bzw. Verarbeitung von Code nicht ausreichend (CWE-94). Ein bereits als Administrator angemeldeter Angreifer kann darüber eigene Befehle einschleusen, die im Kontext des Betriebssystems der Appliance ausgeführt werden. In den beobachteten Angriffen wird die Lücke mit der SSRF-Schwachstelle `CVE-2026-15409` verkettet, um die erforderliche Position auf der Management-Konsole überhaupt zu erreichen.

ANGRIFFSKETTE

01 **AMC erreichbar** – die Appliance Management Console der SMA1000 ist über das Netz ansprechbar

02 **Zugriff verschaffen** – Verkettung mit SSRF (`CVE-2026-15409`), um an die Administrator-Konsole zu gelangen

03 **Code einschleusen** – als Administrator manipulierte Eingabe an den anfälligen AMC-Endpunkt

04 **OS-Befehle ausführen** – beliebige Betriebssystem-Befehle auf der Appliance, faktisch vollständige Übernahme des Gateways

Betroffenheit & Fixversionen

SMA1000-Version	Verwundbar bis	Fixversion (Ziel)
SMA1000 12.4.3	`12.4.3-03245` – `12.4.3-03434`	`12.4.3-03453`
SMA1000 12.5.0	`12.5.0-02283` – `12.5.0-02800`	`12.5.0-02835`
SMA 100-Serie · Firewalls · SMA 500v	nicht betroffen	—

Betroffen ist ausschließlich die SMA1000-Serie (Modelle `SMA6210`, `SMA7210` und die virtuelle `SMA8200v`) in den genannten 12.4.3- und 12.5.0-Ständen. Die separate SMA 100-Serie ist von dieser Schwachstelle nicht betroffen. Die Fixes wurden zunächst als Hotfix über den SonicWall-Support verteilt und ab dem 14. Juli 2026 allgemein bereitgestellt.

Regulatorischer Hinweis: Die kompromittierte Übernahme eines Fernzugangs-Gateways ist regelmäßig ein meldepflichtiger Vorfall: DSGVO unverzüglich (i. d. R. 72 h) bei Betroffenheit personenbezogener Daten, NIS-2 nach den für Sie geltenden Fristen. Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

vor 14.07.2026
Aktive Ausnutzung als Zero-Day, verkettet mit CVE-2026-15409 (SSRF)

14.07.2026
SonicWall veröffentlicht Advisory SNWLID-2026-0008; Hotfixes allgemein verfügbar

14.07.2026
Aufnahme in den CISA-KEV-Katalog (aktive Ausnutzung bestätigt)

offen
NVD-Bewertung ausstehend (Status „Received“, kein CVSS-Basiswert veröffentlicht)

Ihr Maßnahmenplan.

In dieser Reihenfolge – Betroffenheit klären, Hotfix einspielen, Kompromittierung ausschließen, Geheimnisse zurücksetzen.

SOFORT	KURZFRISTIG	BEI BEFUND
Hotfix einspielen / Support kontaktieren	Kompromittierung prüfen (IoC)	Neu aufsetzen · Passwörter & TOTP zurücksetzen

01 Betroffenheit feststellen

Prüfen, ob eine SMA1000-Appliance (`SMA6210`, `SMA7210`, `SMA8200v`) im Einsatz ist und in einem Stand zwischen `12.4.3-03245` und `12.4.3-03434` bzw. `12.5.0-02283` und `12.5.0-02800` läuft.

02 Angriffsfläche verkleinern

Den Zugriff auf die Appliance Management Console (AMC) strikt auf autorisierte Administratoren, Hosts und Netze begrenzen. Die AMC darf nicht breit aus dem Internet erreichbar sein.

03 Hotfix einspielen

Auf `12.4.3-03453` bzw. `12.5.0-02835` oder neuer aktualisieren. Ist der Fix noch nicht verfügbar, den SonicWall-Support wegen des Hotfixes kontaktieren.

04 Kompromittierung ausschließen

Da die Lücke aktiv als Zero-Day ausgenutzt wurde, die Appliance- und Zugriffs-Logs auf ungewöhnliche Administrator-Aktivität und untypische AMC-Zugriffe prüfen. Auch die verkettete Schwachstelle `CVE-2026-15409` berücksichtigen.

05 Bei Verdacht neu aufsetzen und Geheimnisse zurücksetzen

Liegen Kompromittierungshinweise vor, empfiehlt der Hersteller Hardware neu zu imagen bzw. virtuelle Appliances neu auszurollen, alle Benutzer- und Administrator-Passwörter zu ändern und die TOTP-Token zurückzusetzen.

Kompromittierungs-Indikatoren (IoCs)

VERDÄCHTIGE AKTIVITÄT

Ungewöhnliche Administrator-Anmeldungen und untypische Zugriffe auf die AMC-Oberfläche

CHAIN-INDIKATOR

Auffällige interne Anfragen der Appliance (SSRF via `CVE-2026-15409`) vor Befehlsausführung

FOLGEINDIKATOREN

Unerwartete Prozesse/OS-Befehle auf der Appliance · manipulierte Konten oder TOTP-Token

Zur Einordnung: SonicWall hat bis Redaktionsschluss keine eindeutigen, veröffentlichten IoC-Hashes/-Adressen genannt. Da die Ausnutzung Administrator-Kontext voraussetzt und über reguläre AMC-Funktionen läuft, ist sie ohne detaillierte Appliance- und Zugriffs-Logs schwer zu erkennen – bei Verdacht empfiehlt der Hersteller, die Appliance vorsorglich neu aufzusetzen.

Wichtig: Die eigentliche Gefahr entsteht durch die Verkettung: CVE-2026-15410 verlangt für sich genommen bereits Administrator-Rechte (daher „nur“ HOCH statt KRITISCH), wird in den beobachteten Angriffen aber mit der kritischen SSRF-Lücke CVE-2026-15409 kombiniert, um genau diese Rechte zu erlangen. Beide Schwachstellen sollten daher gemeinsam und sofort behandelt werden. Ein offizieller CVSS-Basiswert steht noch aus – die Priorität ergibt sich aus der bestätigten aktiven Ausnutzung (KEV), nicht aus der Zahl.

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 Administrator-Zugriffe auf die AMC und ungewöhnliche OS-Befehle bzw. interne Anfragen der SMA1000-Appliance fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden aus dem Netz erreichbare, 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 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

- Zugriff auf die SMA1000-Management-Konsole heute einschränken; Hotfix 12.4.3-03453 bzw. 12.5.0-02835 unverzüglich einspielen (ggf. über SonicWall-Support).
- CVE-2026-15410 gemeinsam mit der verketteten SSRF-Lücke CVE-2026-15409 behandeln – beide werden aktiv ausgenutzt.
- Bei Kompromittierungshinweisen Appliance neu aufsetzen sowie alle Passwörter und TOTP-Token zurücksetzen – 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-2026-15410 und dem SMA1000-Perimeter.

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

Termin buchen

Quellen: SonicWall PSIRT Advisory SNWLID-2026-0008 (CVE-2026-15410, verkettet mit CVE-2026-15409) · NVD CVE-2026-15410 (Status „Received“, CWE-94; CVSS-Basiswert noch nicht bereitgestellt) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 14.07.2026) · Help Net Security (Herstellereinstufung „High“, betroffene/Fix-Versionen). Der angegebene CVSS-Wert 7,2 (CVSS 3.1) ist eine konservative Argos-Einschätzung, da weder NVD noch PSIRT bislang einen offiziellen Basiswert veröffentlicht haben; gegen das Hersteller-Advisory abgleichen, sobald ein Score vorliegt. Angaben nach bestem Wissen zum Stand 14.07.2026. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.