AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-15409

Unauthentifizierte SSRF in SonicWall SMA1000.

Ein nicht authentifizierter Angreifer aus dem Netz kann die SMA1000-Appliance über das „Work Place“-Interface dazu bringen, Anfragen an von ihm bestimmte, unbeabsichtigte Ziele zu senden – eine Server-Side Request Forgery. In den bislang beobachteten Angriffen wird die Lücke gemeinsam mit der Code-Injection-Schwachstelle CVE-2026-15410 in der Management Console verkettet, um die Appliance vollständig zu kompromittieren. SonicWall bestätigt aktive Ausnutzung; CISA hat die Schwachstelle am 14. Juli 2026 in den KEV-Katalog aufgenommen. Der Hersteller weist ausdrücklich darauf hin, dass ein Patch allein nicht ausreicht.

Geschäftsrisiko: Übernahme des Remote-Access-Gateways, das den Fernzugang ins Unternehmensnetz absichert – mit Potenzial für unbefugten Netzzugriff, Datenabfluss, Betriebsunterbrechung und einen meldepflichtigen Sicherheitsvorfall nach NIS-2 / DSGVO.

10,0 / 10

KRITISCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | Hoch | Kritisch

`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` – aus dem Netz, ohne Anmeldung und ohne Zutun des Nutzers – die Appliance lässt sich dazu bringen, Anfragen an unbeabsichtigte, auch interne Ziele zu senden. In Verkettung mit der Code-Injection-Lücke CVE-2026-15410 in der Management Console droht die vollständige Übernahme des Geräts. Der Basiswert 10,0 stammt aus dem SonicWall-PSIRT-Advisory (SNWLID-2026-0008); eine NVD-Bewertung liegt noch nicht vor (Status „Received“).

AUSGENUTZT SEIT	BETROFFEN	HANDLUNGSBEDARF
14. Juli 2026 (Zero-Day)	SMA1000 12.4.3-03245–03434 · 12.5.0-02283–02800	Sofort

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS 3.1 (SonicWall PSIRT)

Unauth SSRF
ohne Anmeldung aus dem Netz

Aktiv
ausgenutzt · CISA KEV (14.07.2026)

CWE-918
Server-Side Request Forgery

Die Ursache: Das Work-Place-Interface der SMA1000-Appliance validiert in den betroffenen Versionen eine vom Angreifer beeinflussbare Ziel-URL nicht ausreichend, bevor die Appliance selbst eine Anfrage dorthin absetzt. Ein nicht authentifizierter Angreifer kann das Gerät so veranlassen, HTTP-Anfragen an unbeabsichtigte – insbesondere interne – Ziele zu senden (Server-Side Request Forgery, CWE-918). In den beobachteten Angriffen wird dies mit der Code-Injection-Lücke `CVE-2026-15410` in der Management Console kombiniert, um Betriebssystembefehle auszuführen und die Appliance zu übernehmen.

ANGRIFFSKETTE

01
Appliance exponiert – das SMA1000 Work-Place-Interface ist aus dem Internet erreichbar

02
SSRF auslösen – eine manipulierte, unauthentifizierte Anfrage bringt die Appliance dazu, Anfragen an unbeabsichtigte, interne Ziele zu senden

03
Verketten – zusammen mit der Code-Injection-Lücke `CVE-2026-15410` in der Management Console

04
Übernahme – Ausführung von Betriebssystembefehlen und vollständige Kompromittierung der Appliance samt Zugängen ins Netz

Betroffenheit & Fixversionen

SMA1000-Firmware	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 · SonicOS-Firewalls	nicht betroffen	—

Betroffen ist ausschließlich die SMA1000-Serie (Appliances `SMA6210`, `SMA7210`, `SMA8200v`) in den genannten Firmware-Bereichen. Die SMA-100-Serie und die SonicOS-Firewalls sind von dieser Schwachstelle nicht betroffen. Die Fix-Builds `12.4.3-03453` und `12.5.0-02835` wurden vorab als Hotfix über den SonicWall-Support und am 14. Juli 2026 über die SonicWall-Website bereitgestellt.

Regulatorischer Hinweis: Ein bestätigter unbefugter Zugriff über das Remote-Access-Gateway oder ein Abfluss personenbezogener Daten 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

vorab
SonicWall informiert betroffene Kunden und stellt Hotfixes über den Support bereit

14.07.2026
SonicWall veröffentlicht Advisory SNWLID-2026-0008; Fixes in 12.4.3-03453 / 12.5.0-02835

14.07.2026
CISA nimmt CVE-2026-15409 in den KEV-Katalog auf – aktive Ausnutzung

17.07.2026
KEV-Frist für US-Behörden zum Patchen/Abschalten

Ihr Maßnahmenplan.

In dieser Reihenfolge – Zugriff einschränken, Hotfix einspielen, Kompromittierung ausschließen, Zugangsdaten zurücksetzen.

SOFORT	KURZFRISTIG	PARALLEL
Internet-Zugriff einschränken / Hotfix einspielen	Kompromittierung prüfen, ggf. neu aufsetzen	Passwörter & TOTP/MFA zurücksetzen

01 Betroffenheit feststellen

Prüfen, ob eine SMA1000-Appliance (`SMA6210`, `SMA7210`, `SMA8200v`) in einer Firmware zwischen `12.4.3-03245` und `12.4.3-03434` oder zwischen `12.5.0-02283` und `12.5.0-02800` im Einsatz und aus dem Internet erreichbar ist.

02 Sofort mitigieren (vor dem Patch)

Den Zugriff auf das Work-Place-Interface und die Management Console strikt auf autorisierte Nutzer, Hosts und Netze begrenzen bzw. aus dem öffentlichen Internet entfernen. Den Hotfix bei Bedarf über den SonicWall-Support anfordern.

03 Patchen

Auf `12.4.3-03453` bzw. `12.5.0-02835` oder neuer aktualisieren. Wichtig: SonicWall betont ausdrücklich, dass der Patch allein nicht genügt – die folgenden Schritte sind Pflicht.

04 Kompromittierung ausschließen

Zugriffs- und Systemlogs auf anomale Anfragen an das Work-Place-Interface und die Management Console prüfen. Bei Anzeichen einer Kompromittierung die Appliance neu aufsetzen (re-image); SonicWall stellt hierfür ein Prüf-/Bereinigungs-Skript bereit.

05 Zugangsdaten zurücksetzen

Nach dem Patch alle Passwörter sowie die TOTP-/MFA-Seeds der Appliance-Konten zurücksetzen – ein Update macht bereits abgeflossene Geheimnisse nicht ungültig. Von SonicWall ausdrücklich empfohlen.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE AKTIVITÄT	FOLGEINDIKATOREN	VERKETTUNG
Unauthentifizierte Anfragen an das Work-Place-Interface aus fremden Quellen	Ausgehende Anfragen der Appliance an unerwartete interne oder externe Ziele	Anomale Kommandoausführung über die Management Console (`CVE-2026-15410`)

Zur Einordnung: Da die SSRF über reguläre Web-Anfragen läuft, ist sie ohne detaillierte Zugriffs-Logs schwer zu erkennen. SonicWall weist darauf hin, dass ein Patch allein nicht ausreicht – bei Verdacht die Appliance neu aufsetzen und Zugangsdaten zurücksetzen. Der zuverlässigste Nachweis ist die Auswertung Ihrer Zugriffs- und Appliance-Logs.

Wichtig: Der Kern des Risikos liegt in der Verkettung: Die SSRF öffnet ohne Anmeldung den Weg, die Code-Injection-Lücke CVE-2026-15410 vollendet die Übernahme. Deshalb betont SonicWall, dass Patchen allein nicht genügt – kompromittierte Geräte müssen neu aufgesetzt und alle Zugangsdaten samt MFA-Seeds zurückgesetzt werden.

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 Anfragen an das SMA1000-Interface, unerwartete ausgehende Anfragen der Appliance und darüber ausgelöste Kommandoausführung 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 SMA1000-Appliances 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

- Internet-Zugriff auf betroffene SMA1000-Appliances heute einschränken und den Hotfix (12.4.3-03453 / 12.5.0-02835) unverzüglich einspielen.
- Jede betroffene Appliance auf Kompromittierung prüfen und im Verdachtsfall neu aufsetzen lassen – ein Patch allein reicht laut Hersteller nicht.
- Alle Passwörter und TOTP/MFA-Seeds der Appliance zurücksetzen und den Vorfall für eine etwaige Meldung dokumentieren.

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-2026-15409 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-2026-15409) · CVE-CNA-Record SonicWall via CVE Services (CVSS 3.1: 10,0 / Vektor AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H, CWE-918) · NVD (Status „Received“, noch keine eigene CVSS-Bewertung) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 14.07.2026, Frist 17.07.2026) · Help Net Security (Fix-Builds 12.4.3-03453 / 12.5.0-02835, aktive Ausnutzung, Verkettung mit CVE-2026-15410). CVSS-Basiswert stammt vom SonicWall-PSIRT/CNA, da die NVD-Analyse noch ausstand. Angaben nach bestem Wissen zum Stand 14.07.2026; Fixversion gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.