AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-83548

Unauthentifizierte SSRF im SMA1000 Work-Place-Interface.

Ein nicht authentifizierter Angreifer aus dem Netz kann das Work-Place-Interface der SMA1000-Appliance über einen unbeabsichtigten Nebenweg als Weiterleitungs-Proxy missbrauchen – eine Server-Side Request Forgery. Damit erreicht er Funktionen und Ziele, die eigentlich nicht von außen erreichbar sein sollten, und kann die Anmeldung vollständig umgehen. In Verkettung mit der Befehls-Injektion CVE-2026-83549 in der Management Console führt das zur Ausführung von Betriebssystembefehlen ohne jede vorherige Anmeldung. SonicWall bestätigt aktive Ausnutzung; CISA hat die Schwachstelle am 2. September 2026 in den KEV-Katalog aufgenommen. Besonders wichtig: Die im Juli 2026 ausgelieferten Fixstände 12.4.3-03453 und 12.5.0-02835 sind hier selbst betroffen – wer damals gepatcht hat, ist nicht geschützt.

Geschäftsrisiko: Übernahme des Remote-Access-Gateways, das den Fernzugang ins Unternehmensnetz absichert – mit Potenzial für unbefugten Netzzugriff, Abfluss von Zugangsdaten und Daten, 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 eines Nutzers – über einen unbeabsichtigten Nebenweg im Work-Place-Interface lässt sich die Appliance als Proxy missbrauchen und dazu bringen, Anfragen an fremdbestimmte, auch interne Ziele zu senden. Der Höchstwert 10,0 ergibt sich aus dem Sprung über die Systemgrenze (Scope Changed): Der Angreifer wirkt über die Appliance hinaus in dahinterliegende Netze. Bewertung und Vektor stammen von SonicWall als CNA; das NVD hat den Eintrag am 03.09.2026 analysiert und die Werte übernommen, ohne eine eigene Bewertung dagegenzusetzen. Das Hersteller-Advisory weist denselben Vektor als CVSS 3.0 aus.

Das Wichtigste in 60 Sekunden.

10,0 · KRITISCH
CVSS 3.1 (SonicWall PSIRT)

Pre-Auth
ohne Anmeldung aus dem Netz

Aktiv
ausgenutzt · CISA KEV (02.09.2026)

CWE-918 · 441
SSRF & unbeabsichtigter Proxy

Die Ursache: Das **Work-Place**-Interface der SMA1000-Appliance eröffnet in den betroffenen Firmwareständen einen **unbeabsichtigten Nebenweg** (unintended alternate access path): Die Appliance nimmt Anfragen entgegen und leitet sie weiter, ohne die Berechtigung des Aufrufers und das Ziel ausreichend zu prüfen. Ein **nicht authentifizierter** Angreifer aus dem Netz kann das Gerät damit als Weiterleitungs-Proxy missbrauchen (Server-Side Request Forgery, `CWE-918`, in Verbindung mit `CWE-441` – unbeabsichtigter Proxy bzw. „Confused Deputy"). Er erreicht so interne Funktionen und Ziele, die von außen gar nicht erreichbar sein sollten – darunter die Appliance Management Console, deren Befehls-Injektion `CVE-2026-83549` normalerweise Administratorrechte voraussetzt. Genau diese Verkettung macht aus einer Weiterleitungslücke eine vollständige Übernahme ohne Anmeldung.

ANGRIFFSKETTE

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

02
Nebenweg nutzen – eine unauthentifizierte Anfrage bringt die Appliance dazu, als Proxy auf fremdbestimmte Ziele weiterzuleiten

03
Verketten – über den Proxy wird die Management Console erreicht und dort `CVE-2026-83549` ausgelöst

04
Übernahme – Ausführung von Betriebssystembefehlen ohne Anmeldung, Zugriff auf Zugangsdaten und das dahinterliegende Netz

Betroffenheit & Fixversionen

SMA1000-Firmware	Verwundbar bis	Fixversion (Ziel)
SMA1000 12.4.3	`12.4.3-03453 und älter`	`12.4.3-03526`
SMA1000 12.5.0	`12.5.0-02835 und älter`	`12.5.0-02952`
SMA 100 Serie · SSL-VPN auf SonicWall-Firewalls	nicht betroffen	—

Betroffen ist ausschließlich die SMA1000-Serie (Modelle `6210`, `7210`, `8200v`) – physisch wie virtuell. Die SMA-100-Serie und das SSL-VPN auf SonicWall-Firewalls sind laut Hersteller nicht betroffen. **Achtung für alle, die im Juli 2026 gepatcht haben:** Die damaligen Fixstände `12.4.3-03453` und `12.5.0-02835` bilden hier die **obere Grenze des verwundbaren Bereichs** – sie sind also selbst angreifbar. Die neuen Hotfixes `12.4.3-03526` und `12.5.0-02952` stehen über `mysonicwall.com` bereit. Einen Workaround gibt es laut SonicWall nicht.

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, Beweissicherung und Dokumentation.

ZEITACHSE

01.09.2026
SonicWall veröffentlicht Advisory SNWLID-2026-0016 (v1.0) und bestätigt aktive

01.09.2026
Veröffentlichung im NVD

02.09.2026
CISA nimmt CVE-2026-83548 in den KEV-Katalog auf – mit

05.09.2026
KEV-Frist für US-Behörden (BOD 26-04) – bereits verstrichen

Ihr Maßnahmenplan.

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

SOFORT	KURZFRISTIG	PARALLEL

01 Betroffenheit feststellen

Prüfen, ob eine SMA1000-Appliance (6210, 7210, 8200v, physisch oder virtuell) mit einer Firmware bis einschließlich `12.4.3-03453` bzw. `12.5.0-02835` im Einsatz und aus dem Internet erreichbar ist. Der Juli-Patchstand schützt hier nicht.

02 Sofort mitigieren (vor dem Patch)

Einen Workaround gibt es laut SonicWall nicht. Bis zum Hotfix daher den Zugriff auf das Work-Place-Interface und die Appliance Management Console strikt auf autorisierte Netze und Hosts begrenzen bzw. aus dem öffentlichen Internet entfernen.

03 Hotfix einspielen

Auf `12.4.3-03526` bzw. `12.5.0-02952` oder neuer aktualisieren (Platform-Hotfix, verfügbar über `mysonicwall.com`). Wichtig: Der Hersteller macht die folgenden Schritte ausdrücklich zur Pflicht – der Hotfix allein genügt nicht.

04 Kompromittierung ausschließen

Zugriffs- und Systemlogs auf unauthentifizierte Anfragen an das Work-Place-Interface und auf anomale Aktivität in der Management Console prüfen. SonicWall bittet ausdrücklich darum, den technischen Support zur gemeinsamen IoC-Prüfung einzubeziehen. Bei Fund: Hardware neu aufsetzen (re-image), virtuelle Appliances neu ausrollen.

05 Zugangsdaten zurücksetzen

Alle Benutzer- und Administrator-Passwörter der Appliance ändern und die TOTP-Token zurücksetzen – vom Hersteller ausdrücklich verlangt. Ein Update macht bereits abgeflossene Geheimnisse nicht ungültig.

Kompromittierungs-Indikatoren (IoCs)

AUFFÄLLIGE AKTIVITÄT

Unauthentifizierte Anfragen an das Work-Place-Interface aus fremden Quellen

PROXY-MISSBRAUCH

Weiterleitungen der Appliance an unerwartete interne oder externe Ziele

VERKETTUNG

Anomale Kommandoausführung in der Management Console (`CVE-2026-83549`)

Zur Einordnung: Weder SonicWall noch CISA haben öffentliche Indikatoren (IP-Adressen, Hashes, Signaturen) veröffentlicht; ein öffentlicher Exploit-Code war zum Redaktionsschluss ebenfalls nicht bekannt. Da der Angriff über regulär aussehende Web-Anfragen läuft, ist er ohne detaillierte Zugriffs-Logs kaum zu erkennen. Der belastbarste Weg ist deshalb die vom Hersteller angebotene gemeinsame IoC-Prüfung mit dem SonicWall-Support plus die Auswertung Ihrer eigenen Appliance- und Perimeter-Logs. CISA hat für diese Schwachstelle ausdrücklich eine forensische Triage angeordnet – das unterstreicht, dass Patchen allein nicht als Nachweis der Unversehrtheit gilt.

Wichtig: Der Kern des Risikos liegt in der Verkettung: Die SSRF öffnet ohne Anmeldung den Weg bis zur Management Console, die Befehls-Injektion CVE-2026-83549 vollendet die Übernahme. Und die zweite Falle ist der Patchstand: Wer im Juli 2026 auf 12.4.3-03453 oder 12.5.0-02835 aktualisiert hat, sitzt genau auf der obersten verwundbaren Version – ein „ist gepatcht" aus dem Sommer ist hier keine Entwarnung.

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: Unauthentifizierte Anfragen an das Work-Place-Interface, unerwartete Weiterleitungen 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 sofort einschränken und den Hotfix (12.4.3-03526 / 12.5.0-02952) unverzüglich einspielen – ein Workaround existiert nicht.
- Jede betroffene Appliance auf Kompromittierung prüfen lassen, gemeinsam mit dem SonicWall-Support, und im Verdachtsfall neu aufsetzen – die KEV-Frist ist bereits verstrichen.
- Alle Benutzer- und Administrator-Passwörter sowie TOTP-Token zurücksetzen und den Vorgang für eine etwaige Meldung nach NIS-2 / DSGVO 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-2026-83548 und dem SMA1000-Perimeter.

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

Termin buchen

Quellen: SonicWall PSIRT Advisory SNWLID-2026-0016, „SonicWall SMA1000 Series Appliances Affected By Multiple Vulnerabilities" (v1.0, veröffentlicht 01.09.2026; betroffen 12.4.3-03453 und älter / 12.5.0-02835 und älter, behoben in 12.4.3-03526 / 12.5.0-02952; Workaround: keiner; intern entdeckt von William Perry und Adam Babis, SonicWall) · NVD-Eintrag CVE-2026-83548 (veröffentlicht 01.09.2026, Status „Analyzed" 03.09.2026; CVSS 3.1 Basiswert 10,0, Vektor AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H von SonicWall als CNA; CWE-918 und CWE-441) · CISA Known Exploited Vulnerabilities Catalog (aufgenommen 02.09.2026, Frist 05.09.2026 nach BOD 26-04, forensische Triage gefordert, Ransomware-Nutzung „Unknown") · Rapid7 Emergent Threat Response (kein öffentlicher Proof-of-Concept, keine öffentlichen IoCs und keine Zuordnung zu einem Akteur bekannt). Angaben nach bestem Wissen zum Stand 07.09.2026; Fixversion vor dem Einspielen gegen das Hersteller-Advisory abgleichen. Argos Security ist ISO/IEC 27001 (TÜV SÜD) zertifiziert.