AKTIV AUSGENUTZT · CISA KEV

THREAT INTELLIGENCE BRIEFING

CVE-2026-19868

SAML- und MFA-Umgehung im SonicWall SonicOS SSL-VPN.

Wer gültige Zugangsdaten für eine alternative Anmeldemethode besitzt, kann am SonicOS-SSL-VPN die SAML-Kontrollen umgehen – und damit unter Umständen auch die per SAML erzwungene Multi-Faktor-Authentifizierung. CISA führt die Lücke seit dem 6. November 2026 als aktiv ausgenutzt. Einen Workaround gibt es nicht, das Update ist verfügbar.

> **Geschäftsrisiko:** Die MFA ist für viele Unternehmen die zentrale Absicherung des Fernzugangs. Fällt sie aus, kann ein einzelnes entwendetes Passwort für den Zugang reichen – mit dem Risiko eines meldepflichtigen Vorfalls nach NIS-2 / DSGVO.

7,1 / 10

HOCH
CVSS 3.1 BASISWERT

Niedrig | Mittel | **Hoch** | Kritisch

`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:L/A:N` – über das Netz, mit gültigen Zugangsdaten, ohne Zutun eines Nutzers. Kopfwert von SonicWall; CISA-ADP führt im NVD 7,5 ohne vorausgesetzte Rechte (PR:N).

IN CISA KEV SEIT
6. November 2026

BETROFFEN
Gen7 bis 7.3.3-7015 · Gen8 bis 8.2.2-8015
nur mit SAML für SSL-VPN

HANDLUNGSBEDARF
Sofort

Bildmotive: KI-generierte Symbolbilder

Das Wichtigste in 60 Sekunden.

7,1 · HOCH
CVSS 3.1 (SonicWall)

MFA-Bypass
SAML im SSL-VPN · CWE-308

Aktiv
ausgenutzt · CISA KEV · Frist 20.11.2026

Patch da
kein Workaround

Die Ursache: Der SSL-VPN-Dienst von SonicOS setzt die Anmeldung über SAML nicht durchgängig durch (**CWE-308**, einfache statt mehrstufiger Authentifizierung). Ein Nutzer mit gültigen Zugangsdaten für eine **alternative Anmeldemethode** kann so die SAML-Kontrollen umgehen; das kann auch die per SAML erzwungene **MFA** einschließen. Betroffen ist das SSL-VPN nur, wenn SAML dafür aktiviert ist. Technische Details hat SonicWall nicht veröffentlicht.

ANGRIFFSKETTE

01	02	03	04
Ausgangslage – SAML ist für SSL-VPN-Anmeldungen aktiviert	**Zugangsdaten** – gültig für eine alternative Anmeldemethode	**Umgehung** – die SAML-Kontrollen greifen nicht	**Folge** – auch die per SAML erzwungene MFA kann entfallen

Betroffenheit & Fixversionen

Plattform	Verwundbar bis	Fixversion (Ziel)
Gen7 · Hardware + NSv	≤ 7.3.3-7015	7.3.4-7013
Gen8 · Hardware + NSv	≤ 8.2.2-8015	8.2.3-8015
SSL-VPN ohne SAML	nicht betroffen	—

Fixstände laut SonicWall-Advisory **SNWLID-2026-0014** vom 06.11.2026. Gen6 wird dort nicht genannt. Dasselbe Update schließt sechs weitere SonicOS-Lücken, darunter zwei mit CVSS 8,8; als ausgenutzt gelistet ist nur diese.

Regulatorischer Hinweis: Ein unbefugter VPN-Zugriff kann ein meldepflichtiger Sicherheitsvorfall sein – NIS-2 nach den für Sie geltenden Fristen, DSGVO bei personenbezogenen Daten unverzüglich (i. d. R. 72 h). Die Meldung bleibt bei Ihnen; wir unterstützen bei Bewertung und Dokumentation.

ZEITACHSE

06.11.2026
SonicWall-Advisory und Fix

06.11.2026
CVE-Record veröffentlicht

06.11.2026
Aufnahme in CISA KEV

20.11.2026
CISA-Frist für US-Behörden

Bildmotive: KI-generierte Symbolbilder

Ihr Maßnahmenplan.

In dieser Reihenfolge – Betroffenheit klären, patchen, Anmeldungen prüfen.

SOFORT	KURZFRISTIG	PARALLEL
Auf 7.3.4-7013 bzw. 8.2.3-8015	VPN-Anmeldungen prüfen	Anmeldemethoden bereinigen

01 Betroffenheit feststellen

SonicOS-Version aller Gen7- und Gen8-Firewalls einschließlich NSv erheben und prüfen, ob SAML für SSL-VPN-Anmeldungen aktiv ist.

02 Patchen

Auf `7.3.4-7013` (Gen7) bzw. `8.2.3-8015` (Gen8) oder neuer aktualisieren. Einen Workaround nennt SonicWall nicht.

03 Anmeldungen prüfen

SSL-VPN-Anmeldungen suchen, die im Protokoll des Identity Providers kein Gegenstück haben. Das ist unsere Empfehlung, kein Herstellerhinweis.

04 Anmeldemethoden bereinigen

Neben SAML aktive Methoden erfassen und nicht benötigte abschalten. Bei Verdacht betroffene Zugangsdaten zurücksetzen und Sitzungen beenden.

Kompromittierungs-Indikatoren (IoCs)

HERSTELLER-IOCS

Von SonicWall nicht veröffentlicht (Stand 07.11.2026)

PRÜFANSATZ VPN-LOG

Erfolgreiche SSL-VPN-Anmeldung ohne zugehörige Anmeldung am Identity Provider

PRÜFANSATZ KONTEXT

Anmeldungen über alternative Methoden, ungewohnte Quellen und Zeiten

Zur Einordnung: Das sind allgemeine Prüfansätze von Argos, abgeleitet aus der Fehlerbeschreibung, keine bestätigten Indikatoren. Zeitraum, Angreifer und Umfang der Ausnutzung sind nicht veröffentlicht. Ein unauffälliges Ergebnis schließt einen Zugriff daher nicht aus.

Wichtig: Der Patch schließt die Lücke, widerruft aber keine bereits entwendeten Zugangsdaten und klärt keinen erfolgten Zugriff auf. Die Anmeldungen vor dem Update gehören deshalb mit auf den Prüfplan.

Bildmotive: KI-generierte Symbolbilder

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: SSL-VPN-Anmeldungen ohne passendes Ereignis am Identity Provider fallen in unserer Log-Auswertung auf – auch dort, wo interne Teams nicht rund um die Uhr mitlesen.

Vulnerability & Exposure Management

Wir finden SonicOS-SSL-VPN mit aktivem SAML vor 7.3.4-7013 bzw. 8.2.3-8015 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 SonicOS-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

- Heute anordnen: alle Gen7- und Gen8-Firewalls aktualisieren und den Abschluss bestätigen lassen.
- Prüfen lassen, ob vor dem Update auffällige VPN-Anmeldungen stattfanden, und das Ergebnis für eine etwaige Meldung dokumentieren.
- Klären, welche Anmeldemethoden neben SAML am Fernzugang noch aktiv sind und welche davon wirklich gebraucht werden.

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-2026-19868 und dem SonicOS-Perimeter.

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

Termin buchen

Bildmotive: KI-generierte Symbolbilder

Quellen: SonicWall SNWLID-2026-0014 · CVE-Record · NVD · CISA KEV (06.11.2026, Frist 20.11.2026) · BleepingComputer. Stand 07.11.2026 – gegen das Hersteller-Advisory abgleichen.