



Schwachstellen in SonicWall Firewalls mit SonicOS

Der Hersteller SonicWall hat einen Sicherheitshinweis (SNWLID-2025-0016) veröffentlicht, welche eine Schwachstelle in der SonicOS-Software beschreibt. Diese betrifft die SSLVPN-Komponente in Firewalls. Die Lücke könnte einem nicht authentifizierten Angreifer aus der Ferne ermöglichen, einen Denial-of-Service (DoS) zu verursachen, der zum Absturz einer betroffenen Firewall führen kann. Die Sicherheitslücke betrifft verschiedene SonicWall-Hardwareprodukte und stellt ein Risiko für die Netzwerksicherheit dar.

Um was geht es?

Bei der Advisory SNWLID-2025-0016 handelt es sich um eine **Stack-basierte Buffer-Overflow-Schwachstelle** im SSL-VPN-Dienst von SonicOS.

Ein Angreifer ohne vorherige Authentifizierung kann über das Netzwerk eine speziell gestaltete Anfrage senden und damit einen Denial-of-Service (DoS) auslösen – das betroffene Gerät (Firewall) könnte abstürzen.

Im Zusammenhang mit dieser Sicherheitslücke wurden nach Angaben vom Hersteller noch keine verdächtigen Aktivitäten festgestellt.

Details zur Schwachstelle:

Advisory ID SNWLID-2025-0003

CVE CVE-2025-40601

CWE CWE-121

CVSS v3 7.5

CVSS Vec

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Betroffene Produkte	Betroffene Version	Korrigierte Version
Gen7 Firewall series	7.3.0-7012 und älter (7.0.1 Branch nicht betroffen)	7.3.1-7013
Gen8 Firewall series	8.0.2-8011 and older versions	8.0.3-8011

Wie ist die Bedrohungslage auf meiner Anlage?

Falls Sie eine betroffene SonicWall-Firewall einsetzen, hängt die konkrete Bedrohungslage stark von Ihrer Konfiguration und der Netzwerkeexposition ab.

Das Risiko ist deutlich kleiner, wenn **GEO-IP-Filter, Quell-IP-Beschränkungen** oder **eingeschränkte SSL-VPN-Zugänge** aktiv sind.

Bei einem gezielten Angriff auf diese Sicherheitslücke können folgende Auswirkungen auftreten:

- **Einfrieren der Firewall** (Dienst blockiert)
- **Unkontrollierter Neustart der Firewall**
- Während des Neustarts sind die **Netzwerkzonen, oder Teile davon, nicht verfügbar**, was zu Störungen, Prozessunterbrüchen oder Alarmmeldungen führen kann.

Besonders gefährdet sind Systeme, die:

- den **SSL-VPN-Dienst öffentlich** (WAN) anbieten,
- **keine Quell-IP-Beschränkungen** oder GEO-IP-Filter verwenden,
- eine **betroffene SonicOS-Version** einsetzen und noch **nicht gepatcht** wurden.

Wie kann ich mich dagegen schützen?

SonicWall hat ein Update veröffentlicht, das die identifizierten Schwachstellen behebt.

Es wird empfohlen, dieses Update zu installieren, um Ihre Systeme zu sichern.

Aktualisieren Sie die Firmware:

- Installieren Sie die von SonicWall bereitgestellten Firmware-Updates, um die Sicherheitslücke zu schliessen.

Zugriffsbeschränkungen:

- Zugriff nur für vertrauenswürdige Quell-IP-Adressen zulassen

Für Unterstützung können Sie sich kostenpflichtig an die Hotline unter **0844 11 22 11** wenden. Wenn Sie den Update-Service nutzen, entfallen die Kosten.

Update Service

Jedes System sollte regelmässig aktualisiert werden, um es gegen neu entdeckte Schwachstellen zu schützen. Gerade bei einer Firewall empfehlen wir Ihnen einen regelmässigen Software-Update, da es sich um die wichtigste Sicherheitskomponente am Perimeter des Netzwerks zum Schutz ihres Netzwerkes handelt.

Mit unserem Service stellen wir sicher, dass Ihre Systeme regelmässig geprüft, optimiert und aktualisiert werden. So bleibt Ihre Netzwerksicherheit stets auf dem neuesten Stand.

