



## Schwachstelle in SonicWall Firewalls mit SonicOS

Der Hersteller SonicWall hat einen Sicherheitshinweis (SNWLID-2025-0009) veröffentlicht, welche über eine Schwachstelle in der SonicOS-Software informiert. Diese Schwachstelle betrifft die SSLVPN-Komponente. Angreifer könnten über die Schwachstelle die Firewall zum Absturz bringen und so eine Denial-of-Service (DoS)-Situation provozieren. Die Sicherheitslücke betrifft verschiedene SonicWall-Hardwareprodukte und stellt ein erhöhtes Risiko für die Netzwerksicherheit dar.

### Um was geht es?

Der Hersteller SonicWall hat eine Sicherheitslücke in der SSLVPN-Komponente der SonicOS-Firewall-Firmware gemeldet.

Die Schwachstelle wird vom Hersteller als hohes Risiko eingestuft.

Angreifer können sie ausnutzen, um die Firewall aus der Ferne durch eine sogenannte Null Pointer Dereference zum Absturz zu bringen. Dies kann zu einer Denial-of-Service (DoS)-Situation führen, bei der die Firewall zeitweise oder dauerhaft nicht mehr verfügbar ist.

Ein Firmware-Update, welche diese Schwachstelle behebt, wurde vom Hersteller bereitgestellt. Eine zeitnahe Installation wird empfohlen, um die betroffenen Systeme zu schützen.

### Details zur Schwachstelle:

<b>Advisory ID</b>	<a href="#">SNWLID-2025-0009</a>
<b>CVE</b>	CVE-2025-32818
<b>CWE</b>	CWE-476
<b>CVSS v3</b>	7.5
<b>CVSS Vector</b>	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID	Betroffene Produkte	Korrigierte Version
<b>CVE-2025-32818</b>	Gen7 NSv, Gen7 Firewalls	7.2.0-7015 and higher
<b>CVE-2025-32818</b>	TZ80	8.0.1-8017 and higher

### Wie ist die Bedrohungslage auf meiner Anlage?

Die Bedrohungslage ist hoch. Angreifer könnten die Sicherheitslücke ausnutzen um:

- Die Firewall aus der Ferne zum Absturz zu bringen und damit einen Denial-of-Service (DoS) herbeizuführen,
- den Zugriff auf wichtige Netzwerkdienste zu stören oder zu verhindern,
- möglicherweise Folgeangriffe zu erleichtern, wenn die Firewall nach einem Absturz nicht ordnungsgemäss neu startet oder Schutzmechanismen ausfallen.

Besonders gefährdet sind Systeme, die:

- Direkten Internetzugang haben.
- Keine aktuellen Sicherheitsupdates installiert haben.
- Fehlende Schutzmechanismen wie Multi-Faktor-Authentifizierung aufweisen.

### Wie kann ich mich dagegen schützen?

SonicWall hat ein korrigiertes Update der Firmware veröffentlicht, dass die identifizierte Schwachstelle behebt.

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

**Aktualisieren Sie die Firmware:** Installieren Sie die von Sonicwall bereitgestellten Firmware-Updates, um die Sicherheitslücke zu schliessen.

### Multi-Faktor-Authentifizierung aktivieren:

Schützen Sie Ihre Systeme durch die zusätzliche Sicherheitsebene der Multi-Faktor-Authentifizierung vor unbefugtem Zugriff.

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 eine wichtige 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.

