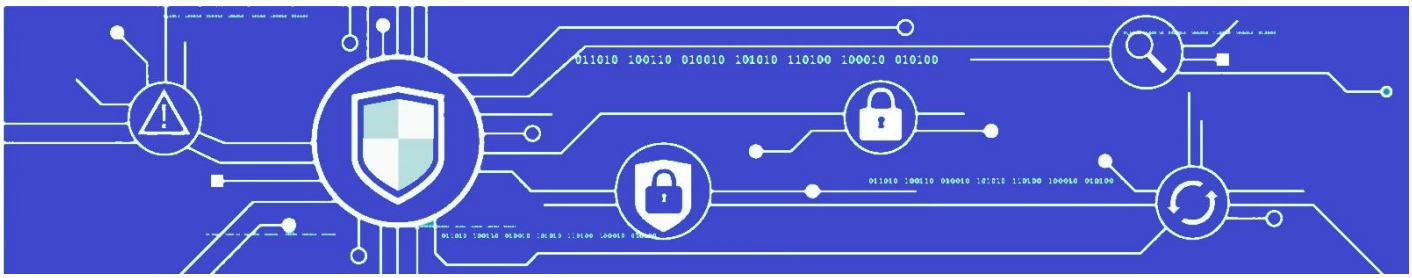

Schwachstellen in SonicWall Firewalls mit SonicOS

Der Hersteller SonicWall hat einen Sicherheitshinweis (SNWLID-2025-0003) veröffentlicht, welcher mehrere Schwachstellen in der SonicOS-Software beschreibt. Diese betreffen insbesondere die SSLVPN-Komponente und das SSH-Management. Angreifer könnten diese Schwachstellen ausnutzen, um Authentifizierungsmechanismen zu umgehen und unbefugte Verbindungen aufzubauen. Die Sicherheitslücken betreffen verschiedene SonicWall-Hardwareprodukte und stellen ein erhebliches Risiko für die Netzwerksicherheit dar.

Um was geht es?

Insgesamt wurden vier Sicherheitslücken identifiziert, die durch das Update behoben werden. Dazu zählen eine Schwachstelle, die eine Umgehung der Authentifizierung im SSL-VPN ermöglicht, sowie eine Lücke, die eine Eskalation von Benutzerrechten bis hin zu Root-Zugriff in den SSH-Konfigurationsfunktionen erlaubt. Zudem wurde eine Server-Side-Request-Forgery im SSH-Management entdeckt. Diese Schwachstellen stellen erhebliche Risiken für die Sicherheit der betroffenen Systeme dar.

Schwachstellen Details:

Advisory ID SNWLID-2025-0003
CVE CVE-2024-40762, CVE-2024-53704, CVE-2024-53705, CVE-2024-53706
CWE CWE-338, CWE-287, CWE-918, CWE-269
CVSS v3 8.2
CVSS Vec VSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

CVE ID	Betroffene Produkte	Korrigierte Version
CVE-2024-40762	Gen6 and Gen7 Firewall series	7.0.1-5165 oder höher
CVE-2024-53704	Gen6 and Gen7 Firewall series	7.1.3-7015 oder höher
CVE-2024-53705	Gen6 and Gen7 Firewalls	7.0.1-5165 oder höher
CVE-2024-53706	Gen7 Cloud NSv	7.1.3-7015 oder höher

Wie ist die Bedrohungslage auf meiner Anlage?

Die Bedrohungslage ist hoch. Angreifer können die Sicherheitslücken ausnützen um:

- Authentifizierungsmechanismen zu umgehen und sich unberechtigten Zugriff auf Systeme zu verschaffen.
- Systemrechte auszudehnen und administrative Kontrolle zu erlangen.
- Zugriff auf sensible Bereiche der Infrastruktur zu erhalten und weitere Angriffe auszuführen.

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 Update veröffentlicht, das die identifizierten Schwachstellen behebt.

Es wird dringend 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.

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.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity

Publiziert: 09/01/2025