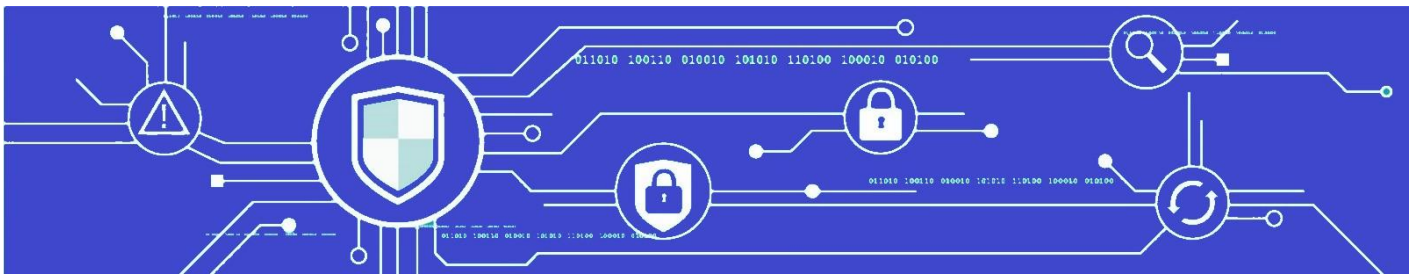

Schwachstelle in SonicWall Firewalls mit SonicOS

Der Hersteller SonicWall hat ein Advisory zu einer kritischen Schwachstelle (CVE-2024-40766) im Betriebssystem SonicOS veröffentlicht, das in Firewalls zum Einsatz kommt. Die Schwachstelle betrifft unter anderem die SSLVPN-Komponente und ermöglicht es Angreifern, die Firewall zum Absturz zu bringen und unter bestimmten Umständen Zugriff auf sensible Ressourcen zu erlangen. SonicWall hat mittlerweile Updates bereitgestellt, die die Lücke schliessen, und empfiehlt, diese umgehend zu installieren.

Um was geht es?

Eine kritische Sicherheitslücke betrifft Firewalls von Sonicwall mit dem Betriebssystem SonicOS. Die Schwachstelle befindet sich in der Zugriffskontrolle sowie in der SSLVPN-Komponente. Unter bestimmten Bedingungen kann dies zum Absturz der Firewall und zu unautorisiertem Zugriff auf Ressourcen führen. Betroffen sind Geräte der Serien Gen5 und Gen6 sowie Gen7 mit älteren Firmware-Versionen.

Schwachstelle Details:

CVE	CVE-2024-40766
CWE	CWE-284: Improper Access Control
CVSS v3	9.3 (HIGH)
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:L

Die Schwachstellen sind gemäss Hersteller ab folgenden Versionen geschlossen:

5.9.2.14-13o (Gen5)
6.5.2.8-2n (für SM9800, NSsp 12400, NSsp 12800)
6.5.4.15.116n (Gen6)
Firmwares aktueller als 7.0.1-5035 (Gen7)

Wie ist die Bedrohungslage auf meiner Anlage?

Die Schwachstelle ermöglicht es einem Angreifer, die Firewall zum Absturz zu bringen, was den Fernzugriff, die Verwaltung und den Betrieb des Systems beeinträchtigen kann. Darüber hinaus besteht die Gefahr, dass der Angreifer unberechtigten Zugriff auf die Firewall erhält und sich von dort aus weiter im Netzwerk und auf andere Systeme ausbreiten kann. Die Verbreitung von Schadsoftware, Datendiebstahl oder die Manipulation von Systemen können so zu weitergehenden Sicherheitsvorfällen führen.

Wie kann ich mich dagegen schützen?

SonicWall hat ein Update bereitgestellt, das diese Schwachstelle behebt.

Es wird empfohlen dieses Update so schnell wie möglich zu installieren, um Ihre Systeme zu schützen.

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

Passwörter ändern: Ändern Sie die Passwörter der SSLVPN-Nutzer, um unbefugten Zugang zu verhindern.

Multi-Faktor-Authentifizierung aktivieren: Aktivieren Sie die Multi-Faktor-Authentifizierung für zusätzliche Sicherheit.

Unterstützung erhalten Sie über die kostenpflichtige Hotline **0844 11 22 11**. Wenn Sie unseren Update-Service nutzen, entfallen die Kosten.

Update-Service
Jedes System sollte regelmässig aktualisiert werden, um es vor neu entdeckten Schwachstellen zu schützen. Insbesondere bei einer Firewall empfehlen wir ein regelmässiges Software-Update, da es sich um die wichtigste Netzwerksicherheitskomponente zum Schutz Ihres Netzwerkes handelt.

Mit dem Update-Service übernimmt Rittmeyer periodisch die Sicherheitsüberprüfung, das Testen und das Einspielen der Software-Updates.

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