



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

0-day Schwachstelle der SonicWall Secure Mobile Access Serie

CSW-Nr. 2021-180976-1331, Version 1.3, 03.02.2021

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) liegen Informationen vor, dass eine 0-day Schwachstellen in der **Secure Mobile Access (SMA) 100 Serie** des Herstellers SonicWall vorliegt.

SonicWall bietet Cybersicherheitsprodukte, -Dienste und -Lösungen, an. SonicWall bestätigte zuletzt, dass man einen koordinierten Angriff auf die eigene Infrastruktur identifiziert hat. Dabei kamen allem Anschein nach Zero-Day-Schwachstellen für bestimmte SonicWall Remote Access Produkte zum Einsatz [SON2021a].

Betroffen sind laut dem Hersteller lediglich Produkte der SMA 100 Serie (SMA 200, SMA 210, SMA 400, SMA 410 und SMA 500v).

Die folgenden Produkte sind demnach **nicht betroffen**:

- SonicWall Firewalls
Alle Generationen von SonicWall-Firewalls sind von der 0-day Schwachstelle der Secure Mobile Access (SMA) 100 Serie nicht betroffen. Kunden oder Partner müssen keine Maßnahmen ergreifen.
- der NetExtender VPN Client
Während zunächst eine Verwundbarkeit von NetExtender 10.X kommuniziert wurde, wird eine solche nun von SonicWall ausgeschlossen. Demnach kann der Client mit allen SonicWall-Produkten verwendet werden.
- die SMA 1000 Serie
Diese Produktlinie ist von diesem Vorfall nicht betroffen. Kunden können die Secure Mobile Access (SMA) 1000 Serie und die zugehörigen Kunden sicher verwenden. Kunden oder Partner müssen keine Maßnahmen ergreifen.
- SonicWave Access Points
Kunden oder Partner müssen keine Maßnahmen ergreifen.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.

2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.

3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.

4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Update 2:

Am 31. Januar meldete die NCC Group an SonicWall eine bereits aktiv ausgenutzte 0-Day-Schwachstelle der SMA 100 Serie [TWI2021].

Am 01. Februar bestätigte SonicWall die 0-Day Schwachstelle in der SMA 100 Serie (SMA 200, SMA 210, SMA 400, SMA 410, SMA 500v) mit Firmwareversion 10.x. Ein Sicherheitspatch ist für den 2. Februar angekündigt und kann nach deutscher Zeit voraussichtlich in der Nacht auf den 3. Februar von der Webseite des Herstellers heruntergeladen werden [SON2021a].

Update 3:

Am 03. Februar teilte SonicWalls Entwicklerteam mit, dass es sich noch in der Finalisierung der neuen Firmwareversion 10.x für die SMA 100-Serie befindet. Nach den Schätzungen des Entwicklerteams ist der Sicherheitspatch für den 3. Februar angekündigt und kann nach deutscher Zeit voraussichtlich am Abend des 04. Februars von der Webseite des Herstellers heruntergeladen werden [SON2021a].

Bewertung

Da es sich um Schwachstellen in einem Sicherheitsprodukt handelt, stuft das BSI die Schwachstellen grundsätzlich als kritisch ein. Außer dem SonicWall selbst betreffenden Vorfall sind dem BSI momentan keine weiteren Fälle bekannt. Der Vorfall wird seitens SonicWall nach wie vor analysiert. Somit ist davon auszugehen, dass SonicWall kurzfristig weitere Details in einem KB-Artikel veröffentlicht [SON2021d].

Maßnahmen

Das BSI empfiehlt Nutzern der SMA 100 Serie, die vom Gerätehersteller empfohlenen Maßnahmen zeitnah umzusetzen. Hierzu gehört die Einschaltung des Time-Based One Time Password (TOTP) für die Zwei-Faktor-Authentifizierung [SON2021b].

Um den Zugriff auf Geräte der SMA 100 Serie weiter abzusichern, sollten Administratoren der SMA 100 Serie zusätzlich zur Implementierung der Zwei-Faktor-Authentifizierung die Umsetzung der seitens Hersteller genannten Maßnahmen prüfen [SON2021c]:

- Aktivieren Sie die Geo-IP / Botnet-Filterung und erstellen Sie eine Richtlinie, die den Webverkehr aus Ländern blockiert, die nicht auf Ihre Anwendungen zugreifen müssen. Weitere Informationen dazu sind auf der S. 248 des SonicWalls Secure Mobile Access 10.2 Administration Guide zu finden.
- Aktivieren und konfigurieren Sie End Point Control (EPC), um das Gerät eines Benutzers zu überprüfen, bevor Sie eine Verbindung herstellen (siehe S. 207 des SonicWalls Secure Mobile Access 10.2 Administration Guide).
- Beschränken Sie den Zugriff auf das SonicWall Portal, indem Sie geplante Anmeldungen / Abmeldungen aktivieren (siehe Seite 117 des SonicWalls Secure Mobile Access 10.2 Administration Guide).

Weitere Informationen zur Einrichtung eines sicheren Fernzugriffs auf das interne Netz stellt das BSI im Rahmen der ISi-Reihe zur Verfügung [BSI2020].

Update 2:

Zum Schutz vor der neu gemeldeten 0-Day-Schwachstelle, empfiehlt das BSI Nutzern der SMA 100 Serie die Umsetzung einer der von SonicWall genannten Maßnahmen:

1. Sofern der SMA 100 eine Firewall vorgeschaltet ist, sind Zugriffe von außen nach Möglichkeit vollständig zu blockieren.
2. Alternativ dazu kann die SMA 100 auch bis zur Verfügbarkeit des angekündigten Patches kurzfristig abgeschaltet werden.
3. Nach einem Factory-Reset kann als dritte Alternative mitunter auch die ältere Firmwareversion 9.x installiert werden. **Bitte sichern Sie zuvor noch unter Version 10.x alle Einstellungen.**

1. Hierbei ist zu beachten, dass ein direktes Downgrade von Firmwareversion 10.x auf 9.x inklusive Konfiguration nicht unterstützt wird. Nach einem Factory-Reset können lediglich zuvor gesicherte 9.x Einstellungen importiert oder das SMA 100 Gerät komplett neu konfiguriert werden.
2. Bei Installation der Version 9.x muss zudem Zwei-Faktor-Authentifizierung gemäß SonicWall's Best-Practice Empfehlungen konfiguriert werden.

Für eine mögliche Detektion von Angriffsversuchen kann in Log-Daten auf von unzulässigen Quellen ausgehende Zugriffe auf das Management Interface gesucht werden.

SonicWall stellt erweiterte Sicherheitsempfehlungen für die SMA 100 Serie zur Verfügung [SON2021e].

Update 3:

Um sich weiterhin vor der 0-Day-Schwachstelle zu schützen, empfiehlt das BSI Nutzern der SMA 100 Serie die empfohlenen Maßnahmen von SonicWall umzusetzen:

SonicWall stellt allen registrierten Geräten der SMA 100-Serie mit der Firmwareversion 10.X-Code die Funktion Web Application Firewall (WAF)-Aktivierung 60-Tage kostenlos zur Verfügung, um die Mitigationsmaßnahmen umsetzen zu können. Diese 60-Tage-Lizenz wird vor Ende des 2. Februars automatisch auf den Konten von registrierten Geräten der SMA 100-Serie aktiviert.

Sicherheitsempfehlungen, wie sie die Web Application Firewall (WAF)-Funktionalität auf der SMA 100-Serie aktivieren können, finden sie in den Anweisungen im folgenden KB-Artikel [SON2021f].

Links

[BSI2020] - Sicherer Fernzugriff auf das interne Netz (ISi-Fern) - Technische Langfassung für IT-Fachkräfte
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi_fern_leitlinie_pdf.pdf?__blob=publicationFile&v=1

[SON2021a] - SonicWall Urgent Security Notice SMA 100 Series
<https://www.sonicwall.com/support/product-notification/urgent-security-notice-sonicwall-confirms-sma-100-series-10-x-zero-day-vulnerability-feb-3-6-a-m-cst/210122173415410/>

[SON2021b] - SonicWall How can I configure Time-Based One Time Password (TOTP) in SMA 100 Series
<https://www.sonicwall.com/support/knowledge-base/how-can-i-configure-time-based-one-time-password-totp-in-sma-100-series/180818071301745/>

[SON2021c] - SonicWall Secure Mobile Access 10.2 Administration Guide
https://www.sonicwall.com/techdocs/pdf/232-005398-00_RevA_SMA_10.2_AdministrationGuide.pdf

[SON2021d] - SonicWall Vulnerability PSIRT SNWLID-2021-0001
<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001>

[SON2021e] - SonicWall Secure Mobile Access (SMA) 100-Series Security Best-Practice Guide
<https://www.sonicwall.com/techdocs/pdf/SMA-100-Series-Security-Best-Practices-Guide.pdf>

[SON2021f] - SonicWall How to Configure Web Application Firewall (WAF) on the SMA 100 Series
<https://www.sonicwall.com/support/knowledge-base/how-to-configure-web-application-firewall-waf-on-the-sma-100-series/210202202221923/>

[TWI2021] - NCC Group Research & Technology SonicWall Tweet
<https://twitter.com/NCCGroupInfosec/status/1355850304596680705>