Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

SonicWall SonicOS: Kritische Schwachstelle erlaubt unauthentifizierten Zugriff auf sensible Ressourcen

Nr. 2024-274200-1022, Version 1.0, 06.09.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 22. August 2024 veröffentlichte der Hersteller SonicWall ein Advisory [SONI24a] zu einer kritischen Schwachstelle im Betriebssystem SonicOS, das u.a. in verschiedenen Firewalls zum Einsatz kommt. Die Sicherheitslücke CVE-2024-40766 soll es Angreifenden durch unsachgemäße Zugriffskontrolle (CWE-284) ermöglichen, ohne Authentifizierung Zugriff auf sensible Ressourcen zu erlangen und unter bestimmten Umständen Firewalls zum Absturz bringen zu können. Nach dem Common Vulnerability Scoring System (CVSS) wurde die Verwundbarkeit mit 9.3 ("kritisch") bewertet und betrifft den Management- und SSLVPN-Zugriff.

Betroffen sind folgende Firewalls:

- SOHO (Gen 5) Firewalls mit der SonicOS Version 5.9.2.14-12o oder älter
- Gen 6 Firewalls (*SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM*

* 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.

9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W) mit der SonicOS Version 6.5.4.14-109n oder älter

- Gen 7 Firewalls (*TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700*) mit der SonicOS Version 7.0.1-5035 oder älter

Am 6. September ergänzte der Hersteller sein Advisory [SONI24a] um den Hinweis, dass möglicherweise **bereits Ausnutzungen der Schwachstelle stattfinden** und ebenfalls der SSLVPN-Zugriff betroffen sei. Weitere Details sind bislang nicht bekannt.

Bewertung

Firewalls sind eine zentrale Sicherheitskomponente für IT-Infrastrukturen und daher ein attraktives Ziel für Angreifende, um Zugriff auf interne Netzwerke zu erlangen und weiterführende Angriffe durchzuführen. Eine Kompromittierung oder ein Ausfall einer Firewall können zu starken Beeinträchtigungen von Geschäftsprozessen führen. Es ist daher sehr wichtig, Schwachstellen in diesen Produkte entsprechend schnell zu patchen und die Produkte sicher zu konfigurieren.

Die möglicherweise bereits beobachteten Ausnutzungen lassen auf weitere zeitnahe, breitflächigere Angriffe auf ungepatchte Firewalls schließen, die SSLVPN oder den WAN-Zugriff auf das Firewall-Management aus dem Internet erlauben.

Der Hersteller SonicWall hat die absichernde Version für Gen 7 Firewalls bereits 2022 veröffentlicht, weshalb Betreiber dieser Firewall Generation bei regelmäßigen Patchen nicht von der Schwachstelle CVE-2024-40766 betroffen sind.

Die Patches für Gen 5 und Gen 6 Firewalls sind jedoch erst kürzlich erschienen und daher womöglich noch nicht auf allen Geräten installiert.

Maßnahmen

IT-Sicherheitsverantwortliche sollten schnellstmöglich die Patchstände auf betriebenen SonicWall-Firewalls prüfen und – sofern erforderlich – die auf mysonicwall.com verfügbaren Updates auf verwundbaren Geräten installieren.

Folgende Versionen sichern die Firewalls ab:

- Für SOHO (Gen 5) Firewalls die SonicOS Version 5.9.2.14-13o oder höher.
- Für Gen 6 Firewalls die SonicOS Version 6.5.2.8-2n (für SM9800, NSsp 12400, NSsp 12800) und 6.5.4.15.116n (für die anderen Gen6 Firewall Appliances).
- Für Gen 7 Firewalls konnte ab der SonicOS Version 7.0.1-5035 (bereits 2022 erschienen) die Schwachstelle nicht reproduziert werden, es sollte jedoch die neuste Version installiert werden.

Der Hersteller SonicWall gibt neben dem Installieren der zur Verfügung stehenden Patches ergänzende Sicherheitsmaßnahmen an, die ebenso als Workaround dienen können, bis der entsprechende Patch installiert wurde. So sollte der Zugriff auf das Management der Firewall nur aus vertrauenswürdigen Quellen erlaubt sein und der WAN-Zugriff generell deaktiviert werden (siehe [SONI24b]). Ebenfalls sollte als Workaround sichergestellt werden, dass der SSLVPN-Zugriff nur aus vertrauenswürdigen Quellen erlaubt bzw. über das Internet deaktiviert ist (siehe [SONI24c]).

Das BSI empfiehlt grundsätzlich, alle Administrations- und Managementzugänge der Firewall auf einzelne vertrauenswürdige Quell-IP-Adressen bzw. -Adressbereiche zu beschränken und den WAN-Zugriff zu deaktivieren (siehe IT-Grundschutzbaustein NET.3.2 Firewall [BSI23]).

SonicWall empfiehlt seinen Kunden, die Gen 5- und Gen 6 Firewalls mit lokalen SSLVPN-Benutzern einsetzen, umgehend die **Passwörter zu wechseln**, um einen unbefugten Zugriff zu verhindern. Administratoren können den Passwortwechsel erzwingen, indem sie die Option "User must change password" für jeden lokalen Account aktivieren.

- Administratoren von Gen 5 Firewalls finden eine Anleitung dafür auf Seite 1340-1341 des SonicOS 5.9-Administratorhandbuchs [SONI24d].
- Administratoren von Gen 6 Firewalls finden eine Anleitung auf Seite 227-228 des SonicOS 6.5-Administratorhandbuchs [SONI24e].

Es ist jedoch bislang unklar, ob Passwörter durch die Schwachstelle abfließen könnten, weshalb das BSI zusätzlich empfiehlt, Kennwörter von lokalen SSLVPN-Benutzern manuell zu wechseln und nicht auf den Passwortwechsel durch die Nutzer für- womöglich bereits kompromittierte - Benutzeraccounts zu warten.

Generell sollte für alle SSLVPN-Benutzer die Multi-Faktor Authentifizierung (MFA) aktiviert werden. Eine Anleitung wird dazu vom Hersteller bereitgestellt, siehe [SONI24f].

Zum aktuellen Zeitpunkt liegen keine weiteren Erkenntnisse über die Ausnutzungen sowie keine Indikatoren zur Feststellung einer Kompromittierung vor.

Links

[SONI24a] SonicWall Security Advisory - CVE-2024-40766
https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0015

[SONI24b] SonicWall - How can I restrict admin access to the device?
https://www.sonicwall.com/support/knowledge-base/how-can-i-restrict-admin-access-to-the-device/170503259079248

[SONI24c] SonicWall - How can I setup SSL-VPN?
https://www.sonicwall.com/support/knowledge-base/how-can-i-setup-ssl-vpn/170505609285133

[SONI24d] SonicWall SonicOS 5.9 Admin Guide
https://www.sonicwall.com/techdocs/pdf/sonicos-5-9-admin-guide.pdf

[SONI24e] SonicWall SonicOS 6.5 Admin Guide
https://www.sonicwall.com/techdocs/pdf/sonicos-6-5-system-setup.pdf

[SONI24f] SonicWall - How do I configure 2FA for SSL VPN with TOTP?
https://www.sonicwall.com/support/knowledge-base/how-do-i-configure-2fa-for-ssl-vpn-with-totp/190829123329169

[BSI23] BSI IT-Grundschutzbaustein - NET.3.2 Firewall (Edition 2023)
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2023.html

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1. Was ist das Traffic Light Protokoll?
   Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
   - **TLP:RED: Persönlich, nur für benannte Empfänger**
     Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
3. Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?
   Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.
4. Was passiert, wenn ich die Einstufung nicht beachte?
   Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.