Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zero-Day-Schwachstelle in SonicWall Email Security Appliance

CSW-Nr. 2021-208213-1132, Version 1.1, 29.04.2021

IT-Bedrohungslage*: 3 / Orange

Sachverhalt

Am 20.04.2021 veröffentlichte die IT-Sicherheitsfirma FireEye einen Bericht über mehrere Zero-Day-Schwachstellen in der SonicWall Email Security Appliance, welche bereits im März 2021 aktiv ausgenutzt wurden [FIR2021].

Diese Schwachstellen ermöglichen einem **nicht authentifizierten** Angreifer die Erstellung eines Accounts mit administrativen Rechten aus der Ferne, sowie die beliebige Ausführung von Code (Remote Code Execution (RCE)).

Für die Schwachstellen wurden die folgenden Common Vulnerabilities and Exposures (CVE)-Nummern registriert:

* 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.

CVE-Kennung	CVSSv3-Wert	Auswirkung
CVE-2021-20021	9.4	Unautorisierte administrative Erstellung eines Benutzeraccounts
CVE-2021-20022	6.7	Beliebiges Hochladen von Dateien nach der Authentifizierung
CVE-2021-20023	6.7	Beliebiges Lesen von Dateien nach der Authentifizierung

Durch diese Schwachstellen in dem Produkt SonicWall E-Mail Security sind sowohl Hardware-Systeme, virtuelle Instanzen, sowie VMware Elastic Sky X integrated (ESXi) und Software-Installationen auf Microsoft-Servern betroffen.

Update 1:
Mit dem vorliegenden Update wurden verschiedene textliche und inhaltliche Anpassungen vorgenommen.

Bewertung

Das BSI geht aufgrund der branchenübergreifenden Verbreitung von einer hohen Betroffenheit aus. Bereits in der Vergangenheit warnte das BSI über verwundbare SonicWall-Systeme mit älteren Schwachstellen.

Da bereits Exploit-Code veröffentlicht wurde, ist zeitnah mit einer breiteren Ausnutzung, bspw. durch Advanced Persistent Threat (APT)-Gruppen, zu rechnen.

Maßnahmen

Das BSI empfiehlt dringend zu überprüfen, ob das betroffene Produkt im Einsatz ist. Um eine Kompromittierung zu verhindern, muss das zur Verfügung stehende Sicherheitsupdate 10.0.9.6173 für Windows User, und das entsprechende Sicherheitsupdate 10.0.9.6177 für Hardware und ESXi Virtuell Appliance User installiert werden. Weitere Informationen zu den Patches können auf der Webseite des Herstellers nachgelesen werden [SON2021].

Insbesondere im Falle von Auffälligkeiten sollte eine weitere mögliche Kompromittierung der internen Netze geprüft werden. Sofern dazu keine internen Ressourcen vorliegen, ist ein externer IT-Forensikdienstleister zu empfehlen [BSI2021]. Im Falle von Angreiferaktivitäten sollten als Mindestanforderung alle Benutzer und Dienstpasswörter zurückgesetzt werden.

Darüber hinaus sollten Security Appliances nicht direkt aus dem Internet erreichbar sein, sondern ausschließlich mittels sicherem Fernzugriff auf das interne Netz verfügbar gemacht werden. Das BSI stellt entsprechende Informationen über das Dokument "Sicherer Fernzugriff auf das interne Netz (ISi-Fern)" zur Verfügung [BSI2020].

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

[BSI2021] - Liste der qualifizierten APT-Response-Dienstleister
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

[FIR2021] - FireEye Blogpost
https://www.fireeye.com/blog/threat-research/2021/04/zero-day-exploits-in-sonicwall-email-security-lead-to-compromise.html

[SON2021] - SonicWall Produkt-Advisory

https://www.sonicwall.com/support/product-notification/security-notice-sonicwall-email-security-zero-day-vulnerabilities/210416112932360/

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 TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. 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. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

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:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.