



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

# SonicWall Network Security Appliance (NSA) Firewall Pufferüberlauf-Schwachstelle CVE-2020-5135

*Ausnutzung erlaubt Denial-of-Service (DoS) und ggf. Remote-Code-Ausführung*

CSW-Nr. 2020-252876-1132, Version 1.1, 23.06.2021

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:WHITE: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE 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

Die SonicWall Network Security Appliance (NSA) ist eine Firewall, die u. a. auch einen SSL VPN Dienst anbietet.

Die Webanwendung der SonicWall Network Security Appliance (NSA) Firewall weist eine Stack-basierte Pufferüberlauf-Schwachstelle (CVE-2020-5135, CVSSv3 9.4/10) auf. Angreifende können mithilfe von präparierten HTTP-Anfragen ohne weitere Authentifizierung einen Denial-of-Service (DoS) der Firewall auslösen. In Kombination mit weiteren Schritten ist ggf. die Remote-Code-Ausführung möglich [TEN2020], [TRI2020].

Folgende SonicOS-Versionen der Firewall sind von der Schwachstelle CVE-2020-5135 betroffen:

- \* 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.

Betroffene SonicOS-Version	SonicOS-Version mit Sicherheitsupdate für CVE-2020-5135
SonicOS 6.5.4.6-79n und vorherige Versionen	SonicOS 6.5.4.7-83n
SonicOS 6.5.1.11-4n und vorherige Versionen	SonicOS 6.5.1.12-1n
SonicOS 6.0.5.3-93o und vorherige Versionen	SonicOS 6.0.5.3-94o
SonicOSv 6.5.4.4-44v-21-794 und vorherige Versionen	SonicOS 6.5.4.v-21s-987
SonicOS 7.0.0.0-1	SonicOS 7.0.0.0-2 und neuere Versionen

Der Hersteller SonicWall stellt ein Sicherheitsupdate zur Behebung der Schwachstelle CVE-2020-5135 zur Verfügung [SON2020].

**Update 1:**

Im Rahmen weiterer Untersuchungen hat ein Sicherheitsforscher herausgefunden, dass das von SonicWall bereitgestellte Update nicht vollständig zielführend ist [TRI2021]. Zwar treten die ursprünglich beobachteten Sachverhalte nicht mehr auf, dafür offenbaren gepatchte SonicWall-Geräte im gleichen Angriffsszenario nun Teile des Speichers. Diese Informationen könnten von Angreifern ggf. für weitere Attacken verwendet werden.

## Bewertung

Die betroffene Webanwendung der SonicWall Network Security Appliance (NSA) Firewall ist bei Nutzung des SSL VPN Dienstes aus dem Internet erreichbar. Es ist daher von einer hohen Anzahl betroffener Systeme auszugehen, in Deutschland sind es alleine über 20.000. Ein DoS der Firewall beeinträchtigt die Verfügbarkeit kritischer Dienste wie z. B. VPN. Die ggf. mögliche Remote-Code-Ausführung in Kombination mit weiteren Schritten gefährdet die Vertraulichkeit und Integrität der Firewall und ggf. weiterer Systeme.

**Update 1:**

Das BSI verfolgt die neuen Entwicklungen mit Sorge: Betreiber könnten sich nach Installation der ursprünglichen Sicherheitsupdates von SonicWall in falscher Sicherheit wiegen. Dies gilt es unbedingt zu vermeiden – insbesondere, da es sich hier um zentrale Netzwerkkomponenten handelt.

## Maßnahmen

Das durch SonicWall zur Verfügung gestellte Sicherheitsupdate [SON2020] zur Behebung der Schwachstelle CVE-2020-5135 sollte umgehend installiert werden. Mit dem Sicherheitsupdate werden zehn weitere Schwachstellen geschlossen [TEN2020].

**Update 1:**

Der Hersteller hat mit neuen Patches für einige Plattformen reagiert. Eine Übersicht über bereitgestellte Sicherheitsupdates für SonicOS ist auf der Webseite von SonicWall zu finden [SON2021]. Angebotene Updates sollten möglichst kurzfristig installiert werden. Betreibern von SonicWall-Produkten, für die derzeit noch keine Patches zur Verfügung stehen, wird empfohlen, die Webseite des Herstellers in den kommenden Tagen regelmäßig auf Updates zu prüfen.

## Links

[SON2020] SonicWall Security Advisory SNWLID-2020-0010  
<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0010>

[TEN2020] CVE-2020-5135: Critical SonicWall VPN Portal Stack-based Buffer Overflow Vulnerability

<https://www.tenable.com/blog/cve-2020-5135-critical-sonicwall-vpn-portal-stack-based-buffer-overflow-vulnerability>

[TRI2020] SonicWall VPN Portal Critical Flaw (CVE-2020-5135)

<https://www.tripwire.com/state-of-security/vert/sonicwall-vpn-portal-critical-flaw-cve-2020-5135/>

[TRI2021] Analyzing SonicWall's Unsuccessful Fix for CVE-2020-5135

<https://www.tripwire.com/state-of-security/featured/analyzing-sonicwalls-unsuccessful-fix-for-cve-2020-5135/>

[SON2021] SonicWall Security Advisory SNWLID-2021-0006

<https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0006>

# 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 sensiblen 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.