



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle mit aktiver Ausnutzung in Fortinet SSL-VPN

CSW-Nr. 2023-240308-1032, Version 1.0, 13.06.2023

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 12. Juni 2023 veröffentlichte das Unternehmen Fortinet ein Security Advisory zu einer kritischen Schwachstelle im SSL-VPN-Dienst von FortiOS und FortiProxy [FORT2023a]. Nach Angaben des Fortinet PSIRT handelt es sich um eine Heap-Speicherüberlaufschwachstelle [CWE122] im SSL-VPN-Dienst. Unautorisierten Angreifenden könnte es demnach gelingen, Schadcode auf dem System oder Befehle über speziell geformte Anfragen auszuführen [FORT2023a].

Die Schwachstelle wird vom Hersteller nach Common Vulnerability Scoring System (CVSS) v3.1 mit einem gesamt CVSS-Wert von 9.2 als „kritisch“ bewertet. Als Kennung wurde die Nummer CVE-2023-27997 vergeben [FORT2023].

Betroffen sind die Produktversionen:

- FortiOS Version 7.2.0 - 7.2.4
- FortiOS Version 7.0.0 - 7.0.11
- FortiOS Version 6.4.0 - 6.4.12
- FortiOS Version 6.2.0 - 6.2.14
- FortiOS Version 6.0.0 - 6.0.16
- FortiOS-6K7K Version 7.0.10

* 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.

- FortiOS-6K7K Version 7.0.5
- FortiOS-6K7K Version 6.4.10 und 6.4.12
- FortiOS-6K7K Version 6.4.2, 6.4.6 und 6.4.8
- FortiOS-6K7K Version 6.2.6, 6.2.7 und 6.2.9 - 6.2.13
- FortiOS-6K7K Version 6.2.4 und 6.2.6 - 6.2.7
- FortiOS-6K7K Version 6.0.10 und 6.0.12 - 6.0.16
- FortiProxy Version 7.2.0 - 7.2.3
- FortiProxy Version 7.0.0 - 7.0.9
- FortiProxy Version 2.0.0 - 2.0.12
- FortiProxy 1.2 alle Versionen
- FortiProxy 1.1 alle Versionen

Möglicherweise sind noch weitere Versionen verwundbar. Eine aktuelle Liste der betroffenen Versionen befindet sich im Advisory [FORT2023a].

Fortinet berichtet, dass die Schwachstelle (CVE-2023-27997) möglicherweise in einer geringen Anzahl an Fällen ausgenutzt wurde [FORT2023b].

Bewertung

Firewalls stellen aufgrund ihrer zentralen Bedeutung als Schutzsystem und ihrer exponierten Position für die IT in Organisationen attraktive Ziele für Cyber-Angriffe dar. Eine Kompromittierung bietet zahlreiche Optionen zur weiteren Ausbreitung in internen Netzwerken und zur Manipulation des Datenverkehrs.

Die Schwachstelle ist als sehr kritisch anzusehen, da sie entfernten Angreifern ermöglicht, Code einzuschleusen und die Authentifizierung inklusive Multi-Faktor-Authentifizierung zu umgehen.

Es ist zu erwarten, dass die Schwachstelle (CVE-2023-27997) zeitnah von Angreifenden auf ungepatchten Systemen ausgenutzt wird, wie in der Vergangenheit bereits in anderen Fällen beobachtet wurde. Da Fortinet selbst von Angriffen berichtet [FORT2023b], ist es wichtig, die Lage im Blick zu halten und die Aktualisierungen schnellstmöglichst einzuspielen.

Maßnahmen

Fortinet hat am 8. Juni 2023 Updates zum Schließen der Schwachstelle bereitgestellt. Es wird empfohlen, eine zeitnahe Aktualisierung auf folgende Versionen vorzunehmen:

- FortiOS Version 7.4.0 oder höher
- FortiOS Version 7.2.5 oder höher
- FortiOS Version 7.0.12 oder höher
- FortiOS Version 6.4.13 oder höher
- FortiOS Version 6.2.15 oder höher
- FortiOS Version 6.0.17 oder höher
- FortiOS-6K7K Version 7.0.12 oder höher
- FortiOS-6K7K Version 6.4.13 oder höher
- FortiOS-6K7K Version 6.2.15 oder höher
- FortiOS-6K7K Version 6.0.17 oder höher

- FortiProxy Version 7.2.4 oder höher
- FortiProxy Version 7.0.10 oder höher
- FortiProxy Version 2.0.13 oder höher

Weitere Empfehlung zur Konfiguration von Firewalls [BSI2021a] und VPN [BSI2021b] können dem BSI IT-Grundschutz-Kompendium entnommen werden.

Links

[FORT2023a] <https://www.fortiguard.com/psirt/FG-IR-23-097>

[FORT2023b] <https://www.fortinet.com/blog/psirt-blogs/analysis-of-cve-2023-27997-and-clarifications-on-volt-typhoon-campaign>

[CWE122] <https://cwe.mitre.org/data/definitions/122.html>

[BSI2021a] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.html

[BSI2021b] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_3_VPN_Edition_2021.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-ingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.