Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

**SCHWACHSTELLE** | GEFÄHRDUNG | VORFALL | IT-ASSETS

# Aktive Ausnutzung einer Schwachstelle in Fortinet SSL-VPN

*CSW-Nr. 2022-283701-1032, Version 1.0, 13.12.2022*

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

Am Abend des 12.12.2022 (deutscher Zeit) veröffentlichte das Unternehmen Fortinet Informationen zu einer kritischen Schwachstelle im SSL-VPN-Dienst von FortiOS (siehe [FORT2022a]). Nach Angaben des Fortinet PSIRT befindet sich eine Speicherüberlaufschwachstelle (Heap-based buffer overflow – siehe [CWE2022]) im SSL-VPN-Dienst von FortiOS, welcher auf FortiGate Firewalls zur Einsatz kommt. Diese Schwachstelle ermöglicht es unautorisierten Angreifenden, Schadcode auf dem System oder Befehle über speziell geformte Anfragen auszuführen.

Die Schwachstelle wird vom Hersteller nach Common Vulnerability Scoring System (CVSS) v3.1 mit einem gesamt CVSS-Wert von 9.3 als „kritisch“ bewertet. Für die Schwachstelle wurde die CVE-2022-42475 vergeben (siehe [FORT2022a], [MITR2022]).

Betroffen sind die Produktversionen:

- FortiOS-6K7K Version 7.0.0 - 7.0.7
- FortiOS-6K7K Version 6.4.0 - 6.4.9
- FortiOS-6K7K Version 6.2.0 - 6.2.11
- FortiOS-6K7K Version 6.0.0 - 6.0.14

* 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 Version 7.2.0 - 7.2.2
- FortiOS Version 7.0.0 - 7.0.8
- FortiOS Version 6.4.0 - 6.4.10
- FortiOS Version 6.2.0 - 6.2.11

Im Rahmen der Veröffentlichung gab der Hersteller außerdem bekannt, dass bereits ein Fall einer erfolgreichen Ausnutzung der Schwachstelle beobachtet wurde. Weitere Details zur Erkennung des beobachteten Angriffs können dem Abschnitt "Maßnahmen" entnommen werden.

# Bewertung

Firewalls stellen aufgrund ihrer zentralen Bedeutung 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. Der bereits beobachtete Angriff unterstreicht diese Bewertung. Es muss damit gerechnet werden, dass weitere Angriffsversuche auf Organisationen stattfinden, die FortiGates betreiben.

# Maßnahmen

Fortinet stellt bereits Patches auf ihrer Webseite zur Verfügung (siehe [FORT2022b]). Empfohlen wird eine zeitnahe Aktualisierung auf

- FortiOS version 7.2.3 oder höher
- FortiOS version 7.0.9 oder höher
- FortiOS version 6.4.11 oder höher
- FortiOS version 6.2.12 oder höher
- FortiOS-6K7K version 7.0.8 oder höher
- FortiOS-6K7K version 6.4.10 oder höher
- FortiOS-6K7K version 6.2.12 oder höher
- FortiOS-6K7K version 6.0.15 oder höher

Unabhängig von den konkreten Schutzmaßnahmen in diesem Sachverhalt sollten IT-Sicherheitsverantwortliche stets dafür sorgen, dass die Patchstände der betriebenen Systeme aktuell sind (siehe [BSI2022]).

Im Rahmen der Veröffentlichung stellte das Unternehmen zusätzliche Indicators of Compromise (IOC) bereit, welche bei dem durch das Unternehmen beobachteten Angriff ermittelt wurden.

Logfiles sollten auf folgende Einträge geprüft werden:
*Logdesc="Application crashed" and msg="[...] application:sslvpnd,[...], Signal 11 received, Backtrace: [...]“*

Für Dateisysteme sollte überprüft werden, ob sich folgende Dateien/Artefakte auf dem System befinden:
*/data/lib/libips.bak*
*/data/lib/libgif.so*
*/data/lib/libiptcp.so*
*/data/lib/libipudp.so*
*/data/lib/libjepg.so*
*/var/.sslvpnconfigbk*
*/data/etc/wxd.conf*
*/flash*

Des Weiteren wurden verdächtige IP Adressen (und Ports) seitens Fortinet identifiziert, die in einem näheren Zusammenhang mit dem Vorfall stehen:
188.34.130.40:444

103.131.189.143:30080,30081,30443,20443
192.36.119.61:8443,444
172.247.168.153:8033

# Links

[BSI2022] BSI IT-Grundschutz – OPS.1.1.3 Patch- undÄnderungsmanagement:
https://bsi.bund.de/dok/989196

[CWE2022] - CWE-122: Heap-based Buffer Overflow:
https://cwe.mitre.org/data/definitions/122.html

[FORT2022a] FortiOS - heap-based buffer overflow in sslvpnd
https://www.fortiguard.com/psirt/FG-IR-22-398

[FORT2022b] Fortinet - Customer & Technical Support:
https://support.fortinet.com

[MITR2022] CVE-2022-42475
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42475

# 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.