Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Schwachstelle in Sicherheitslösungen von Fortinet

Nr. 2022-266664-1022, Version 1.0, 10.10.2022

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 10. Oktober veröffentlichte der IT-Hersteller Fortinet ein Advisory, in dem Nutzer über eine kritische Schwachstelle in den Produkten FortiGate, FortiProxy und FortiSwitchManager informiert werden (siehe [FORT2022]). Demnach könnte es nicht-authentisierten Angreifenden aus der Ferne gelingen, sowohl bei FortiGate, welches FortiOS verwendet, als auch bei FortiProxy und FortiSwitchManager die Authentifizierung auf der administrativen Oberfläche zu umgehen und anschließend Befehle auf dem Gerät auszuführen.

Betroffen sind folgende Softwareversionen bzw. Patch-Stände:

- FortiGate mit FortiOS: Versionen zwischen 7.0.0 und 7.0.6 sowie zwischen 7.2.0 und < 7.2.2
- FortiProxy: Versionen zwischen 7.0.0 und 7.0.6 sowie Version 7.2.0
- FortiSwitchManager: Version 7.0.0 und 7.2.0

Gemäß Common Vulnerability Scoring System (CVSS) wird die Schwachstelle (CVE-2022-40684) mit einem Wert von 9.6 von 10 als "kritisch" eingestuft (siehe [MITRE2022]).

* 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.

Darüber hinaus wies Fortinet darauf hin, dass bereits ein Vorfall beobachtet worden sei, bei dem die Schwachstelle aktiv durch Angreifende ausgenutzt wurde. Hinweise zur Detektion stellt der IT-Hersteller ebenfalls bereit (siehe [FORT2022]).

Bewertung

Für zentrale IT-Komponenten in Organisationen – wie im vorliegenden Fall – besteht grundsätzlich ein erhöhtes Bedrohungspotenzial, da Angreifende von dort ausgehend verschiedene Angriffsszenarien, wie z.B. das Abgreifen von Informationen oder auch die weitere Ausbreitung im Netzwerk, durchführen könnten.

IT-Sicherheitsverantwortliche sollten die Absicherung und Wartung dieser Geräte daher mit erhöhter Priorität verfolgen. Die Beobachtung eines bereits identifizierten Angriffs im vorliegenden Sachverhalt unterstreicht diese Notwendigkeit.

Maßnahmen

Fortinet stellt Softwareupdates zur Verfügung, mit deren Hilfe die Schwachstelle geschlossen wird. IT-Sicherheitsverantwortliche sollten daher schnellstmöglich die Installation folgender Versionen prüfen:

- Für FortiGate mit FortiOS: Upgrade auf 7.0.7 bzw. 7.2.2 oder höher
- Für FortiProxy: Upgrade auf 7.0.7 bzw. 7.2.1 oder höher
- Für FortiSwitchManager: Upgrade auf 7.2.1 oder höher

Darüber hinaus weist der Hersteller auf verschiedene Workarounds hin, die sich zum Teil auch aus den allgemeinen Schutzmaßnahmen für IT in Organisationen nach BSI IT-Grundschutz u.a. ableiten lassen (siehe [BSI2022a], [BSI2022b]). Dies sind insbesondere:

- die Vermeidung der Erreichbarkeit der Administrationsoberfläche aus dem Internet,
- eine Beschränkung des administrativen Zugriffs auf Fortinet Geräte mittels IP-Filter/VPN.

Eine Anleitung zur Anpassung der Konfiguration stellt Fortinet auf seiner Webseite zur Verfügung (siehe [FORT2022]).

Zur Detektion womöglich bereits erfolgter Angriffe sollte in Logs nach Einträgen von user="Local_Process_Access" gesucht werden.

Links

[FORT2022] - FortiOS / FortiProxy / FortiSwitchManager - Authentication bypass on administrative interface:
https://www.fortiguard.com/psirt/FG-IR-22-377

[MITRE2022] - CVE-2022-40684
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-40684

[BSI2022a] - BSI IT-Grundschutz: NET.3.2 Firewall (Edition 2022)
https://bsi.bund.de/dok/989066

[BSI2022b] - BSI IT-Grundschutz:NET.3.3 VPN (Edition 2022)
https://bsi.bund.de/dok/989056

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.