



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Fortinet FortiWeb OS anfällig für Command Injection

CSW-Nr. 2021-243017-1032, Version 1.0, 18.08.2021

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

Am 17. August 2021 berichtete das IT-Sicherheitsunternehmen Rapid7 in seinem Blog über eine Schwachstelle im Management Interface von Fortinets FortiWeb OS [RAP72021]. Die damit verwaltete Web Application Firewall (WAF) Fortinet FortiWeb wird in vielen Organisationen zum Schutz von Webangeboten eingesetzt.

Dem Artikel zufolge kann ein authentifizierter Angreifer die Ausführung von Befehlen auf dem Gerät provozieren (eng. *command injection*) und die WAF somit vollständig übernehmen. In der Folge ist die Installation einer Shell oder von Schadsoftware denkbar. Exploit Code hat Rapid7 ebenfalls in seinem Blog veröffentlicht (vgl. [RAP72021]).

Betroffen sind die **FortiWeb OS Versionen 6.3.11 und älter**. Mit einem CVSS-Score von 8.7 wird die Schwere der Sicherheitslücke als „hoch“ eingestuft. Ein Patch ist aktuell noch nicht verfügbar.

Zusätzliche Brisanz erhält der Sachverhalt in Verbindung mit der im Januar veröffentlichten Schwachstelle CVE-2020-29015 [MITR2021]. Damals war eine Möglichkeit bekannt geworden, die Authentifizierungsmechanismen von Fortinet FortiWeb zu umgehen. Für Geräte, auf denen seit diesem Zeitpunkt keine Updates mehr eingespielt wurden, könnte somit auch die o.g. Einschränkung für die Ausnutzung der nun gefundenen Sicherheitslücke entfallen.

* 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.

Bewertung

Aufgrund der zentralen Bedeutung von Web Application Firewalls für die Sicherheitskonzepte von Webanwendungen geht das BSI im vorliegenden Fall von einer erheblichen Bedrohung aus.

In Zusammenhang mit der schon länger bekannten Schwachstelle CVE-2020-29015 zeigt sich auch einmal mehr, wie Angreifer sich unzureichendes Patchmanagement für die Verkettung mehrerer Sicherheitslücken zu Nutze machen können.

Maßnahmen

Zum aktuellen Zeitpunkt hat Fortinet noch keinen Patch zur Verfügung gestellt.

Betreiber sollten daher Schutzmechanismen etablieren, die einen unerlaubten Zugriff auf das Management Interface verhindern – zum Beispiel durch die Nutzung von VPN. Die ungeschützte Erreichbarkeit aus dem Internet ist in jedem Fall zu vermeiden.

Allgemeine Hinweise zur Absicherung und dem Aufbau von Firewalls stellt das BSI im Grundsatz-Kompendium bereit (siehe [BSI2021]).

Links

[RAP72021] Fortinet FortiWeb OS Command Injection

<https://www.rapid7.com/blog/post/2021/08/17/fortinet-fortiweb-os-command-injection/>

[MITR2021] MITRE CVE Datenbank

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-29015>

[BSI2021] NET.3.2: Firewall (Edition 2021)

[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundsatz/Kompendium Einzel PDFs 2021/09 NET Netze und Kommunikation/NET 3 2 Firewall Edition 2021.pdf](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundsatz/Kompendium_Einzel_PDFs_2021/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2021.pdf)

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.