Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Fortinet FortiOS: Aktive Ausnutzung kritischer Schwachstellen

Nr. 2024-213797-1022, Version 1.0, 09.02.2024

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 8. Februar 2024 veröffentlichte der Hersteller Fortinet ein Advisory [FORTI24a] [BSI2024a] zu einer kritischen Schwachstelle in mehreren Versionen seines Betriebssystems FortiOS, das u.a. in den Firewalls der FortiGate-Serie zum Einsatz kommt.

Bei der gefundenen Sicherheitslücke CVE-2024-21762 handelt es sich um eine Out-of-bounds Write Verwundbarkeit (CWE-787), die einem nicht authentifizierten, externen Angreifenden über präparierte HTTP Anfragen die Ausführung von Code und Befehlen ermöglicht. Nach dem Common Vulnerability Scoring System (CVSS) erhielt die Schwachstelle mit einem Wert von 9.8 eine "kritische" Bewertung.

Fortinet hat Patches für die betroffenen, folgenden Versionen von FortiOS veröffentlicht:

- 7.4.0 bis einschließlich 7.4.2
- 7.2.0 bis einschließlich 7.2.6
- 7.0.0 bis einschließlich 7.0.13
- 6.4.0 bis einschließlich 6.4.14
- 6.2.0 bis einschließlich 6.2.15
- 6.0 alle Versionen

* 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 7.6 Versionen sind nicht betroffen.

Fortinet gibt im Advisory [FORTI24a] an, dass die Schwachstelle **wahrscheinlich schon ausgenutzt wird**. Weitere Begründungen für diese Annahme liefert das Unternehmen zum aktuellen Zeitpunkt nicht.

Außerdem informierte der Hersteller über den Fund einer weiteren kritischen Schwachstelle in FortiOS, die im Rahmen interner Untersuchungen entdeckt wurde [FORTI24b] [BSI2024a]. Hier könnten Angreifende über bestimmte Anfragen beliebigen Code auf Geräten mit FortiOS ausführen. Die Sicherheitslücke wurde mit einem CVSS-Score von 9.8 als "kritisch" bewertet.

Betroffen sind verschiedene Software-Versionen aus den Reihen FortiOS 7.4.x, 7.2.x und 7.0.x, FortiOS 6.x hingegen nicht. Darüber hinaus machte Fortinet hier keine Angabe, ob Annahmen für eine aktive Ausnutzung vorliegen.

Bewertung

Lösungen des Herstellers Fortinet finden sich häufig an zentralen Stellen eines IT-Netzwerks. Dementsprechend stellen diese Produkte grundsätzlich attraktive Ziele für Cyber-Angriffe dar. Auch Berichte über Vorfälle aus der jüngeren Vergangenheit lassen darauf schließen, dass Täter proaktiv nach verwundbaren Fortinet Produkten suchen.

Herstellerunabhängig stellen Firewalls aufgrund ihrer Bedeutung als wesentliche IT-Schutzmaßnahmen für Organisationen auch grundsätzlich attraktive Ziele für Cyber-Angriffe dar.

IT-Sicherheitsverantwortliche sollten die Umsetzung der unten beschriebenen Maßnahmen daher kurzfristig prüfen.

Maßnahmen

IT-Sicherheitsverantwortlichen wird empfohlen, schnellstmöglich zu handeln und die verfügbaren Patches einzuspielen oder den vom Hersteller empfohlenen Workaround anzuwenden. Dabei sollten beide Schwachstellen zeitnah geschlossen werden, auch wenn nur bei einem Sachverhalt Informationen über eine aktive Ausnutzung vorliegen.

Es sollte auf folgende absichernde Versionen aktualisiert werden:

- FortiOS 7.4.3 oder höher
- FortiOS 7.2.7 oder höher
- FortiOS 7.0.14 oder höher
- FortiOS 6.4.15 oder höher
- FortiOS 6.2.16 oder höher

Für FortiOS 6.0 stehen keine Patches zur Verfügung, es muss daher zu einer höheren Version gewechselt werden.

Ebenfalls ist es nach Angaben von Fortinet möglich, die SSL VPN-Funktionalität vorübergehend zu deaktivieren, bis Patches eingespielt werden können, um betroffene Systeme vor Angriffen abzusichern. Die Deaktivierung des Webmodus ist hingegen keine ausreichende Mitigationsmaßnahme.

Weitere Informationen zum sicheren Betrieb von Firewalls können auch dem BSI IT-Grundschutz entnommen werden [BSI2024b].

Links

[FORTI24a] FortiOS - Out-of-bound Write in sslvpnd:
https://fortiguard.fortinet.com/psirt/FG-IR-24-015

[FORTI24b] FortiOS - Format String Bug in fgfmd:
https://fortiguard.fortinet.com/psirt/FG-IR-24-029

[BSI2024a] [WID-SEC-2024-0330] Fortinet FortiOS: Mehrere Schwachstellen ermöglichen Codeausführung:
https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2024-0330

[BSI2024b] BSI IT-Grundschutz – NET.3.2 Firewall:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2023.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 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-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.