Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung von Schwachstellen in F5 BIG-IP

Nr. 2023-283789-1022, Version 1.0, 03.11.2023

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 26. Oktober veröffentlichte F5 zwei Advisories [F5a][F5b] zu Schwachstellen im Konfigurationsprogramm von BIG-IP (all modules). Die Schwachstelle CVE-2023-46747 ermöglicht es entfernten Angreifenden mit Zugriff auf das Traffic Management User Interface (TMUI) beliebigen Code mit Administratoren Privilegien auszuführen. Sie erhielt eine CVSS-Bewertung von 9.8 ("kritisch"). [PRAET23a] [F5a]

Die zweite Schwachstelle CVE-2023-46748 ermöglicht einen authentifizierten Angreifenden mit Zugriff auf TMUI eine SQL-Injection durchzuführen, um System-Befehle auszuführen und wurde mit CVSS-Score von 8.8 ("hoch") bewertet. [F5b]

Die IT-Sicherheitsforschenden von *praetorian* haben zur der Schwachstelle CVE-2023-46747 einen detaillierten technischen Bericht [F5b] veröffentlicht. In diesem wird auf die Ähnlichkeit der Schwachstelle zu CVE-2020-5902 eingegangen, die ebenfalls kurz nach dem Bekanntwerden ausgenutzt wurde, und wie die Sicherheitslücke gefunden wurde. Die Ausnutzung von CVE-2023-46747 wird durch eine ältere Schwachstelle CVE-2022-26377 ermöglicht. Diese wurde zwar von F5 in einem Advisory [F5c] bekannt gegeben, jedoch nicht mit einem Patch behoben. Die Schwachstelle CVE-2022-26377 kann für Request Smuggling ausgenutzt werden und betrifft die in BIG-IP verwendete Apache Version. [PRAET23b]

* 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.

In dem Blogbeitrag des IT-Sicherheitsuntermehmens *tenable* und in den Advisories von F5 wird bereits von beobachteten Ausnutzungen von CVE-2023-46747 und CVE-2023-46748 gesprochen. Ebenfalls wird auf ein öffentlich verfügbares Proof-of-Concept verwiesen. [TENA23]

Betroffen von den Schwachstellen (CVE-2023-46747 und CVE-2023-46748) sind folgende Versionen von BIG-IP:

- BIG-IP 13.x : 13.1.0 - 13.1.5
- BIG-IP 14.x: 14.1.0 - 14.1.5
- BIG-IP 15.x: 15.1.0 - 15.1.10
- BIG-IP 16.x: 16.1.0 - 16.1.4
- BIG-IP 17.x: 17.1.0 - 17.1.1

Bewertung

Weltweit sollen nach dem Blogbeitrag von *praetorian* [PRAET23a] mehr als 6000 Server potentiell bedroht sein, darunter größere Unternehmen und Regierungs-Einrichtungen. Schwachstellen in BIG-IP Produkte von F5 waren bereits in der Vergangenheit von Angreifern schnell ausgenutzt wurden.

Besonders kritisch ist die einfache Ausnutzbarkeit durch die Verfügbarkeit von technischen Details und Proof-of-Concepts. Angreifer benötigen lediglich Zugriff zum Traffic Management User Interface (TMUI), um Geräte vollständig zu kompromittieren.

Maßnahmen

IT-Sicherheitsverantwortliche sollten so schnell wie möglich die verfügbaren Patches einspielen. Details zu den Patches (Versionen) finden sich in den Advisories [F5a][F5b] des Herstellers F5. Ebenfalls findet sich in den Advisories Mitigations-Skripte für BIG-IP Versionen 14.1.0 und höher, welche zur Behebung der Schwachstellen genutzt werden können.

Außerdem sollte, sofern möglich, das BIG-IP Traffic Management User Interface (TMUI) nicht aus dem Internet erreichbar sein. Dies kann auch als vorübergehende Mitigationsmaßnahme dienen, sofern keine Patches zeitnah eingespielt werden können. [F5a]

F5 hat Indikatoren veröffentlicht, die bei der Ausnutzung von CVE-2023-46748 in Kombination mit CVE-2023-46747 beobachtet wurden:

In der Datei */var/log/tomcat/catalina.out* können Einträge ähnlich zu folgenden Zeilen auf eine Kompromittierung hinweisen [F5b]:

> {...}
>
> java.sql.SQLException: Column not found: 0.
>
> {...)
>
> sh: no job control in this shell
>
> sh-4.2$ <EXECUTED SHELL COMMAND>
>
> sh-4.2$ exit.

Wobei die Nummer in der Zeile "Column not found" ebenfalls eine andere sein kann und der ausgeführte Befehl abhängig vom Angriff ist.

Aufgrund der bereits beobachteten Ausnutzung [F5b] sollte auf eine bereits stattgefundene Kompromittierung geprüft werden, falls die TMUI von extern erreichbar war/ist. Bei Verdacht auf eine Kompromittierung eines BIG-IP Systems sollten die Maßnahmen aus dem Guide von F5 [F5d] umgesetzt und das betroffene System schnellst möglichst isoliert werden.

Links

[PRAET23a] https://www.praetorian.com/blog/advisory-f5-big-ip-rce/

[PRAET23b] https://www.praetorian.com/blog/refresh-compromising-f5-big-ip-with-request-smuggling-cve-2023-46747/

[TENA23] https://www.tenable.com/blog/cve-2023-46747-critical-authentication-bypass-vulnerability-in-f5-big-ip

[F5a] Advisory CVE-2023-46747 https://my.f5.com/manage/s/article/K000137353

[F5b] Advisory CVE-2023-46748 https://my.f5.com/manage/s/article/K000137365

[F5c] Advisory CVE-2022-26377 https://my.f5.com/manage/s/article/K000132643

[F5d] Guidance by suspected compromise https://my.f5.com/manage/s/article/K11438344

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.