Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Schwachstelle in Atlassian Confluence

CSW-Nr. 2023-274964-1132, Version 1.1, 11.10.2023

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 4. Oktober veröffentlichte Atlassian ein Advisory [ATLA23a] zu einer kritischen Schwachstelle (CVE-2023-22515) in Confluence Data Center und Server. Die Schwachstelle ermöglicht es entfernten Angreifenden unautorisierte Administrator-Konten zu erstellen und auf Confluence Instanzen zuzugreifen. Die Schwachstelle erhält eine CVSS-Bewertung von 10.0 ("kritisch") [NVD23].

Nach Angaben des Herstellers Atlassian wurde die Schwachstelle möglicherweise bei einigen Kunden bereits aktiv ausgenutzt [ATLA23a].

Die nachfolgenden Versionen des Confluence Data Centers und Confluence Servers sind jeweils von der Sicherheitslücke betroffen:

8.0.0, 8.0.1, 8.0.2, 8.0.3, 8.0.4, 8.1.0, 8.1.1, 8.1.3, 8.1.4, 8.2.0, 8.2.1, 8.2.2, 8.2.3, 8.3.0, 8.3.1, 8.3.2, 8.4.0, 8.4.1, 8.4.2, 8.5.0, 8.5.1

Versionen **unter** dem Patchstand von **8.0.0 sind nicht** von dieser Schwachstelle **betroffen**, ebenso nicht bei Atlassian Cloud gehostete Instanzen (erkennbar an atlassian.net in der Domain).

* 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.

Update 1:
Microsoft Threat Intelligence hat beobachtet, dass die APT Gruppe Storm-0062 (auch unter dem Namen DarkShadow oder Oro0lxy geführt) die Schwachstelle CVE-2023-22515 bereits seit dem 14. September ausnutzt. [TWITT23a]

Bewertung

Die weite Verbreitung von Atlassian Confluence Data Center und Server sowie die dort gespeicherten, mitunter vertraulichen Daten machen die Kollaboration und Wissensmanagement-Lösung zu einem beliebten Ziel bei Angreifenden. Eine Ausweitung der von Atlassian beobachteten Angriffe hält das BSI für wahrscheinlich.

Besonders kritisch ist die **Ausnutzbarkeit von extern**, sollte die Confluence Instanz aus dem Internet erreichbar sein.

Maßnahmen

Atlassian gibt im Advisory zu der Schwachstelle [ATLA23a] Mitigationsmaßnahmen an und stellt Updates zur Verfügung. IT-Sicherheitsverantwortliche sollten so schnell wie möglich Confluence Instanzen aktualisieren oder, falls dies nicht möglich ist, die beschriebenen Mitigationsmaßnahmen des Herstellers umsetzen. Ebenfalls sollte auf eine mögliche, bereits stattgefundene Kompromittierung anhand der bereitgestellten Indikatoren von Atlassian geprüft werden [ATLA23b].

Folgende Versionen von Confluence Data Center und Confluence Server schließen die Schwachstelle (CVE-2023-22515):

- 8.3.3 oder höher
- 8.4.3 oder höher
- 8.5.2 oder höher

Sollte nicht auf eine der gelisteten Versionen aktualisiert werden können, so können folgende Mitigationsmaßnahmen getroffen werden:

- Zwischenzeitlich den externen Netzwerkzugriff auf die Instanz beschränken
- Zusätzlich den Zugriff auf die */setup/** Endpunkte von Confluence blockieren, die zur Ausnutzung der Schwachstelle notwendig sind. Dies kann umgesetzt werden durch:
  - Beschränken des Netzwerkzugriffs auf diesen Pfad oder durch das
  - Anpassen der Confluence Konfigurationsdatei. Hierzu muss die */<confluence-install-dir>/confluence/WEB-INF/web.xml* Dateien angepasst werden und der folgende Codeblock vor dem *</web-app>* Tag am Ende der Datei hinzugefügt werden:

```
<security-constraint>
    <web-resource-collection>
     <url-pattern>/setup/*</url-pattern>
        <http-method-omission>*</http-method-omission>
     </web-resource-collection>
    <auth-constraint />
</security-constraint>
```

Ebenfalls stellt Atlassian folgende Indicators-of-Compromises (IoCs) zur Verfügung, die auf eine bereits stattgefundene Ausnutzung der Schwachstelle hindeuten:

- Nicht autorisierte Teilnehmer in der *confluence-administrators* Gruppe
- Nicht erwartete, neu erstellte Nutzer-Konten
- Anfragen an die */setup/*.action* Endpunkte (sind in den Netzwerk-Logs zu finden)
- Fehlermeldungen, die "*/setup/setupadministrator.action*" enthalten, sind in *atlassian-confluence-security.log* (im Confluence Installations-Ordner) zu finden

Weitere Informationen zu der Schwachstelle stellt Atlassian in einem FAQ [ATLA23b] zur Verfügung.

Update 1:
Microsoft Threat Intelligence hat IPs in einem Twitter Post angegeben, die im Zusammenhang mit den beobachteten Angriffen auf die Schwachstelle stehen. [TWITT23b]

- 192.69.90[.]31
- 104.128.89[.]92
- 23.105.208[.]154
- 199.193.127[.]231

Das Team von Rapid7 konnte die Schwachstelle, neben der im Advisory genannten Endpunkten in */setup/*.action,* ebenso durch */server-info.action* ausnutzen [RAPID7].

Durch die bereits seit 14. September beobachteten Angriffe sollte anhand der Indikatoren geprüft werden, ob eine Kompromittierung möglicherweise bereits vor dem 4. Oktober stattfand.

Bei einer festgestellten Kompromittierung sollte nach Möglichkeit:

1. Eine schnelle Einzelfallbetrachtung mit einem lokalen oder externen IT-Sicherheits-Team durchgeführt werden, bevor Notfallmaßnahmen wie z.B. die Trennung von Netzwerkverbindungen ergriffen werden.
   Ziel wäre dabei u.a. eine Prüfung, ob unter Akzeptanz von Restrisiken laufende Angreiferaktivitäten beobachtet werden können. In einigen Fällen ist nur so das Ausmaß der eigenen Kompromittierung feststellbar. Die dabei potentiell durch Entscheidungsträger zu akzeptierenden Restrisiken für alle Netzwerke, an denen das betroffene System angeschlossen ist, sind vor Akzeptanz genauso zu prüfen wie die zur Beobachtung erforderlichen Sicherheitsmaßnahmen (z.B. erhöhte Detektion, Klärung von Abbruchkriterien).
2. Wenn 1. nicht kurzfristig möglich ist oder sich gegen eine Beobachtung des Angreifers entschieden wurde, sollten betroffene Systeme lediglich vom Netzwerk getrennt werden und nicht ausgeschaltet werden.
3. Falls ein betroffenes System ohne forensische Sicherung ausgeschaltet wird, gehen für die forensische Analyse wichtige Daten unwiederbringlich verloren. Dies kann im schlimmsten Fall die Vorfallsaufklärung verhindern. Deswegen ist der unter 2. beschriebene Schritt aus Sicht des BSI empfehlenswert. Falls ein betroffenes System trotzdem ausgeschaltet werden soll, sollte zuvor eine forensische Sicherung des Systems erfolgen.

Links

[ATLA23a] https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html

[ATLA23b] https://confluence.atlassian.com/kb/faq-for-cve-2023-22515-1295682188.html

[NVD23] https://nvd.nist.gov/vuln/detail/CVE-2023-22515

[TWITT23a] https://twitter.com/msftsecintel/status/1711871732644970856

[TWITT23b] https://twitter.com/MsftSecIntel/status/1711871733932671336

[RAPID7] https://www.rapid7.com/blog/post/2023/10/04/etr-cve-2023-22515-zero-day-privilege-escalation-in-confluence-server-and-data-center/

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.