Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Zeroday-Schwachstelle in Atlassian Confluence

Nr. 2022-232716-1022, Version 1.0, 03.06.2022

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 2. Juni 2022 veröffentlichte das Unternehmen Atlassian ein Advisory zu einer kritischen Sicherheitslücke in seinem Produkt Confluence – einer weit verbreiteten Anwendungen zur Realisierung von Wikis [ATLA2022]. Demnach könnte es einem unauthentifizierten Angreifenden gelingen, aus der Ferne Code auszuführen und eine Webshell zu installieren.

Betroffen sind sowohl das Confluence Data Center als auch Confluence Server. Gemäß Common Vulnerabilities and Exposures (CVE) wird die Schwachstelle unter der Nummer CVE-2022-26134 geführt und als "kritisch" bewertet.

Ein Patch ist noch nicht verfügbar.

Gleichzeitig sind bereits Berichte über eine aktive Ausnutzung der Schwachstelle erschienen. So veröffentlichte das IT-Sicherheitsunternehmen Volexity einen Blogbeitrag zu den Erkenntnissen aus der Analyse eines Angriffs Ende Mai [VOLE2022]. Auch die amerikanische CISA hat die Sicherheitslücke in ihren „Known Exploited Vulnerabilities Catalog“ aufgenommen [CISA2022].

Volexity stellte außerdem eine Liste der IPs zur Verfügung, von denen die Zugriffe auf die Webshells erfolgten:

- 154.146.34.145
- 154.16.105.147

* 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.

- 156.146.34.46
- 156.146.34.52
- 156.146.34.9
- 156.146.56.136
- 198.147.22.148
- 221.178.126.244
- 45.43.19.91
- 59.163.248.170
- 64.64.228.239
- 66.115.182.102
- 66.115.182.111
- 67.149.61.16
- 98.32.230.38

Bewertung

Die weite Verbreitung von Atlassian Confluence, die dort gespeicherten, mitunter nicht zur Veröffentlichung bestimmten Daten und das Fehlen eines Patches führen nach Ansicht des BSI dazu, dass kurzfristig mit weiteren Angriffen zu rechnen ist.

Weiterhin muss davon ausgegangen werden, dass die Liste der bereitgestellten IPs nicht abschließend ist bzw. VPNs zum Einsatz kamen.

Maßnahmen

Da noch kein Patch verfügbar ist, hat Atlassian auf seiner Internetseite zwei Mitigationsmaßnahmen genannt:

1. Einschränkung der Erreichbarkeit von Confluence aus dem Internet.
2. Abschaltung von Confluence Server und Data Center Instanzen.

Sofern diese Maßnahmen nicht möglich sind, kann das Risiko durch die Implementierung einer Regel für die Web Application Firewall gemindert werden: URLs, die die Zeichen "${" enthalten, sollten geblockt werden.

Weiterhin sollten IT-Sicherheitsverantwortliche regelmäßig prüfen, wann das Unternehmen einen Update zur Verfügung stellt.

Darüber hinaus können die von Volexity angebotenen Yara-Regeln [GIT2022] genutzt werden, um die eigenen Systeme auf Webshell-Aktivitäten zu untersuchen.

Links

[ATLA2022] Confluence Security Advisory 2022-06-02
https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

[VOLE2022] Zero-Day Exploitation of Atlassian Confluence
https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/

[CISA2022] Known Exploited Vulnerabilites Catalog
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

[GIT2022] Volexity on GitHub
https://github.com/volexity/threat-intel/blob/main/2022/2022-06-02%20Active%20Exploitation%20Of%20Confluence%200-day/indicators/yara.yar

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.