SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Schwachstelle in Atlassian Confluence Data Center und Server

Nr. 2023-283932-1021, Version 1.0, 07.11.2023

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Am 31. Oktober veröffentlichte Atlassian ein Advisory [ATLA23a] zu einer kritischen Schwachstelle (CVE-2023-22518) in Confluence Data Center und Server. Die Schwachstelle ermöglicht es entfernten unautorisierten Angreifenden Confluence zurückzusetzen und ein Confluence-Instanzadministratorkonto zu erstellen. Mit diesem Konto können Angreifende alle administrativen Aktionen durchführen, die dem Confluence-Instanzadministrator zur Verfügung stehen. Die Schwachstelle wurde anfangs mit einem CVSS-Wert von 9.1 geführt. Im Rahmen der Untersuchungen von Angriffen korrigierte das Unternehmen den CVSS-Wert am 07. November und setze diesen auf die höchste Stufe eine 10.0 ("kritisch") [NVD23][ATLA23a].

Nach Angaben des Herstellers Atlassian sind alle Confluence Data Center und Server Versionen von der Schwachstelle betroffen [ATLA23a][ATLA23b]. Bei Atlassian Cloud gehostete Instanzen (erkennbar an atlassian.net in der Domain) sind nach Angaben des Herstellers nicht betroffen. Zusätzlich bestätigte der Hersteller, dass die Schwachstelle bereits aktiv ausgenutzt wird [ATLA23a].

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. Öffentlich zugängliche Instanzen von Confluence Data Center und Server sind besonders gefährdet und erfordern die sofortige Ergreifung von Maßnahmen.

* 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.

Maßnahmen

Atlassian gibt im Advisory zu der Schwachstelle [ATLA23a] Mitigationsmaßnahmen an und stellt Updates zur Verfügung. IT-Sicherheitsverantwortliche sollten zeitnah 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 [ATLA23a][ATLA23b]. Mit den nachfolgenden Patchversionen wurde die Schwachstelle behoben:

- 7.19.16
- 8.3.4
- 8.4.4
- 8.5.3
- 8.6.1

Nach Angaben des Herstellers können unter anderem die folgenden Indikatoren auf eine Kompromittierung hinweisen:

- Zugriffsverlust auf die Confluence Data Center und Server Instanzen
- Requests mit /jsons/setup-restore* in den Netzwerk-Logs
- Installation unbekannter Plugins
  - Atlassian identifizierte maliziöse Plugins mit dem Namen web.shell.Plugin
- Verschlüsselte Dateien
- Neue (unbekannte) Nutzeraccounts in der Confluence-Administratorengruppe
- Unbekannte neue Nutzeraccounts

Sollten IT-Sicherheitsverantwortliche die aufgeführten Aspekte auf den Instanzen identifizieren, so ist von einer Kompromittierung der Confluence Data Center und Server Instanz auszugehen.

Links

[ATLA23a] Security Advisory CVE-2023-22518
https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html

[ATLA23b] FAQ 2023-22518
https://confluence.atlassian.com/kb/faq-for-cve-2023-22518-1311474094.html

[NVD23] National Vulnerability Database - NVD - CVE-2023-22518
https://nvd.nist.gov/vuln/detail/CVE-2023-22518