The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
06/03/2022

SUBJECT:
A Vulnerability in Atlassian Confluence Server and Data Center Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in Atlassian Confluence Server and Data Center, which could allow for remote code execution. Confluence is a wiki tool used to help teams collaborate and share knowledge efficiently. Successful exploitation of this vulnerability could allow for remote code execution within the context of the service account used to run the Confluence Server or Data Center service. Depending on the privileges associated with the service account, an attacker could view, change, or delete data. If the service account has been configured to have fewer rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

THREAT INTELLIGENCE:
According to open source reporting, cyber threat actors (CTAs) are actively exploiting CVE-2022-26134 in Confluence Server 7.18.0 to install web shells. Cybersecurity firm Volexity used a proof-of-concept exploit to determine that it likely affects all current versions of Confluence. Volexity is working with Atlassian and is not releasing the proof-of-concept exploit at this time. Atlassian states on their website that there are currently no fixed versions of Confluence Server or Data Center.

On June 2, 2022, Volexity released a blog post detailing an incident response investigation involving the zero-day exploitation of CVE-2022-26134. The investigation showed that a CTA achieved unauthenticated remote code execution on Confluence servers via CVE-2022-26134 and loaded a malicious class file in memory that effectively provided a webshell for continued access.

The CTAs deployed an in-memory webshell known as Behinder and then wrote JSP webshells to a publicly accessible web directory. According to Volexity, one of the files was a well-known “copy of the JSP variant of the China Chopper webshell” that “appears to have been written as a means of secondary access.” The CTAs also executed commands on the system that included reconnaissance efforts, dumping a Confluence user table, and removing evidence of exploitation.

CISA recently included CVE-2022-29464 to their list of “Known Exploited Vulnerabilities Catalog” and is requiring federal agencies to block all internet traffic to Confluence servers by today, June 3, 2022.

SYSTEMS AFFECTED:

- Confluence Server (All Supported Versions)
- Confluence Data Center (All Supported Versions)

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in Atlassian Confluence Server and Data Center, which could allow for remote code execution.

Tactic: *Initial Access* **(**TA0001**):**
Technique: *Exploit Public-Facing Application* **(**T1190**):**

- A command injection vulnerability could allow an unauthenticated user to execute remote code on a Confluence Server or Data Center instance. (CVE-2022-26134)

Successful exploitation of this vulnerability could allow for remote code execution within the context of the service account used to run the Confluence Server or Data Center service. Depending on the privileges associated with the service account, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. If this service account has been configured to have fewer rights on the system, exploitation of this vulnerability could have less impact than if it was configured with administrative rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate updates provided by Atlassian once they become available to vulnerable systems immediately after appropriate testing, or **apply an appropriate workaround if an update is not available for your system. Atlassian has recommended restricting internet access to Confluence Server and Data Center instances or disabling them.** (See the Atlassian link below.) (**M1051: Update Software, M1042: Disable or Remove Feature or Program**)
    - **Safeguard 4.8:** Uninstall or Disable Unnecessary Services on Enterprise Assets and Software: Uninstall or disable unnecessary services on enterprise assets and software, such as an unused file sharing service, web application module, or service function.
    - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process**: Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
    - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
- Apply the Principle of Least Privilege to all systems and services. Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack. (**M1026: Privileged Account Management**)
    - **Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:** Manage default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts. Example implementations can include: disabling default accounts or making them unusable.
    - **Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:** Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.
- Use capabilities to prevent suspicious behavior patterns from occurring on endpoint systems. This could include suspicious process, file, API call, etc. behavior. (**M1040 : Behavior Prevention on Endpoint**)
    - **Safeguard 13.2 : Deploy a Host-Based Intrusion Detection Solution**: Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.
    - **Safeguard 13.7 : Deploy a Host-Based Intrusion Prevention Solution:** Deploy a host-based intrusion prevention solution on enterprise assets, where appropriate and/or supported. Example implementations include use of an Endpoint Detection and Response (EDR) client or host-based IPS agent.

REFERENCES:

Atlassian:
https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

Volexity:
https://www.volexity.com/blog/2022/06/02/zero-day-exploitation-of-atlassian-confluence/

Bleeping Computer:
https://www.bleepingcomputer.com/news/security/critical-atlassian-confluence-zero-day-actively-used-in-attacks/

CISA:
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134