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

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

09/03/2021

SUBJECT:

A Vulnerability in Confluence Server and Data Center Could Allow for Arbitrary Code Execution

OVERVIEW:

A vulnerability has been discovered in Confluence Server and Data Center, which could allow for arbitrary code execution. Confluence is a wiki tool used to help teams collaborate and share knowledge efficiently. Successful exploitation of this vulnerability could allow an unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance. Depending on the privileges associated with the instance, an attacker could view, change, or delete data.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Confluence Server and Data Center all versions prior to 6.13.23
- Confluence Server and Data Center versions from 6.14.0 prior to 7.4.11
- Confluence Server and Data Center versions from 7.5.0 prior to 7.11.6
- Confluence Server and Data Center versions 7.12.x prior to 7.12.5

RISK:

Government:

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

Businesses:

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

Home users: NA

TECHNICAL SUMMARY:

A vulnerability has been discovered in Confluence Server and Data Center Could Allow for Arbitrary Code Execution. An OGNL injection could allow an authenticated user, and in some instances an unauthenticated user, to execute arbitrary code on a Confluence Server or Data Center instance. The vulnerable endpoints can only be accessed if 'Allow people to sign up to create there account' is enabled. Successful exploitation of this vulnerability could allow an unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance.

Depending on the privileges associated with the instance, an attacker could view, change, or delete data.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by Atlassian to vulnerable systems immediately after appropriate testing.
- Run all software as a nonprivileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Evaluate read, write, and execute permissions on all newly installed software.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Atlassian:
https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26084