UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00192

CONFLUENCE SERVER & DATA CENTRE VULNERABILITY

DATE ISSUED: 6th September 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	MEDIUM	[✓ EASY]

OVERVIEW

It has been discovered that the popular wiki and collaboration tool Confluence – an Atlassian product – has a critical vulnerability that could allow and unauthenticated user to remotely execute code on the Server or Data Centre instance.

BREAKDOWN

While Confluence Cloud customers are not affected by this vulnerability, and vulnerable endpoints can only be exploited if the 'Allow people to sign up and create a user account' is enabled, there are now reports it is being exploited in the wild. Versions 6.13.23, 7.11.6, 7.12.5, 7.13.0 and 7.4.11 are also unaffected by this bug. All other versions should be patched immediately and have their settings reviewed. The Object-Graph Navigation Language (OGNL) injection vulnerability could allow an unauthorised user to remote execute code, read, modify, and/or delete data dependant on the level of privilege associated with the account. OGNL is an open-source expression language (EL) for Java objects and exploitation is possible when the EL interpreter attempts to decipher user-supplied data without validation allowing the attacker to input their own code.

REMEDIATION STEPS

- Apply latest security patches and updates provided by Atlassian. If you are unable to upgrade immediately, Atlassian have also provided a temporary workaround. (See resources below)
- Have software running in non-privileged user mode (rather than with administrator privileges) to reduce the potential effects of a successful attack.
- When deploying new software always check read, write, and execute permissions and apply the principle of Least Privilege to all systems and services.

REFERENCES & RESOURCES

Atlassian	https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html
Mitre	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-26084
CIS Advisory	