Security Advisory 2021-046

Critical Vulnerability in Confluence

September 1, 2021 — v1.0

TLP:WHITE

History:

- *01/09/2021 — v1.0 – Initial publication*

Summary

On 25th of August 2021, Atlassian released a Confluence Security Advisory regarding Confluence Server Webwork OGNL injection [1]. Atlassian rates the severity level of this vulnerability as critical. There is no CVSS score provided yet [2].

Technical Details

An OGNL injection vulnerability exists that would allow an authenticated user, and in some instances unauthenticated user, to execute arbitrary code on a Confluence Server or Data Center instance. The issue is tracked in [3].

Products Affected

Confluence Server and Data Center versions before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5 are affected by this vulnerability [1].

Recommendations

Atlassian recommends that you upgrade to the latest Long Term Support release [1]. CERT-EU recommends updating the vulnerable application as soon as possible.

Workarounds and Mitigations

If you are unable to upgrade Confluence immediately, then as a temporary workaround, the issue can be mitigate by running scripts provided by Atlasian [1].

References

[1] https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html

[2] https://nvd.nist.gov/vuln/detail/CVE-2021-26084

[3] https://jira.atlassian.com/browse/CONFSERVER-67940