Vulnerabilities in Atlassian Products

February 21, 2024 — v1.0

TLP:CLEAR

History:

- *21/02/2024 — v1.0 – Initial publication*

Summary

On February 20, 2024, Atlassian released a security advisory addressing a high severity vulnerability in Confluence Data Center and Confluence Server that, if exploited, could allow an authenticated attacker to execute arbitrary HTML or JavaScript code on a victim's browser [1]. The security advisory also addresses 10 other high severity vulnerabilities which have been fixed in new versions of several Atlassian products [2].

Technical Details

The vulnerability `CVE-2024-21678`, with a CVSS score of 8.5, is a stored XSS vulnerability that allows an authenticated attacker to execute arbitrary HTML or JavaScript code on a victim's browser which has a high impact to confidentiality, low impact to integrity, no impact to availability, and requires no user interaction. [1].

Among the other 10 vulnerabilities [2], 9 of them allow an unauthenticated attacker to expose assets in the environment susceptible to exploitation which might have an impact to confidentiality, integrity, or availability, and requires no user interaction.

Affected Products

The vulnerability `CVE-2024-21678` affects the following versions of Confluence Data Center, and Confluence Server

- from 8.7.0 to 8.7.1 (only Confluence Data Center)
- from 8.6.0 to 8.6.1 (only Confluence Data Center)
- from 8.5.0 to 8.5.4 LTS
- from 8.4.0 to 8.4.5
- from 8.3.0 to 8.3.4
- from 8.2.0 to 8.2.3
- from 8.1.0 to 8.1.4
- from 8.0.0 to 8.0.4
- from 7.20.0 to 7.20.3
- from 7.19.0 to 7.19.17 LTS
- from 7.18.0 to 7.18.3

- from 7.17.0 to 7.17.5
- Any earlier versions

The other 10 high severity vulnerabilities affect several products of Atlassian. A complete list can be found on the vendor's website [2].

Recommendations

CERT-EU strongly recommends installing the latest version of Atlassian products as soon as possible.

References

[1] https://jira.atlassian.com/browse/CONFSERVER-94513

[2] https://confluence.atlassian.com/security/security-bulletin-february-20-2024-1354501606.html