CERT-EU 10 years

Security Advisory 2024-009

Critical and High Vulnerabilities in Atlassian Products

January 17, 2024 — v1.0

TLP:CLEAR

History:

- *17/01/2024 — v1.0 – Initial publication*

Summary

On January 16, 2024, Atlassian released a security advisory addressing a critical vulnerability in Confluence Data Center and Confluence Server that, if exploited, could lead to Remote Code Execution (RCE) on the affected server [1].

The editor also released a security advisory addressing 28 high-severity vulnerabilities which have been fixed in new versions of Atlassian products [2].

Technical Details

The critical vulnerability `CVE-2023-22527`, with a CVSS score of 10, is due to a template injection vulnerability on out-of-date versions of Confluence Data Center and Server that allows an unauthenticated attacker to achieve RCE on an affected version [1].

Among the other 28 vulnerabilities [2], 6 of them could lead to Remote Code Execution on several Atlassian products.

Affected Products

The vulnerability `CVE-2023-22527` affects out-of-date Confluence Data Center and Server 8 versions released before Dec. 5, 2023 (i.e., Confluence Data Center and Server versions 8.0.x, 8.1.x, 8.2.x, 8.3.x, 8.4.x, 8.5.0-8.5.3), as well as 8.4.5 which no longer receives backported fixes in accordance with Atlassian's Security Bug Fix Policy [1].

The other 28 vulnerabilities affect [2]:

- Bitbucket Data Center before versions 7.21.21, 8.9.9, 8.13.5, 8.14.4, 8.15.3, 8.16.2 and 8.17.0;
- Bitbucket Server before versions 7.21.21, 8.9.9, 8.13.5 and 8.14.4;
- Bamboo Data Center and Server before versions 9.2.9, 9.3.6 and 9.4.2;
- Jira Data Center and Server before versions 9.4.13 and 9.7.0;
- Jira Service Management Data Center and Server before versions 4.20.30, 5.4.15 and 5.12.2;

- Crowd Data Center and Server before the version 5.2.2;
- Confluence Data Center before versions 7.19.18, 8.5.5 and 8.7.2;
- Confluence Server before versions 7.19.18 and 8.5.5.

Recommendations

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

References

[1] https://confluence.atlassian.com/security/cve-2023-22527-rce-remote-code-execution-vulnerability-in-confluence-data-center-and-confluence-server-1333990257.html

[2] https://confluence.atlassian.com/security/security-bulletin-january-16-2024-1333335615.html