Security Advisory 2024-029

Vulnerabilities in Atlassian Products

March 20, 2024 — v1.0

TLP:CLEAR

History:

- *20/03/2024 — v1.0 – Initial publication*

Summary

On March 19, 2024, Atlassian released a security advisory addressing 24 high and critical vulnerabilities, among which a critical severity vulnerability in Bamboo Data Center/Server and a high vulnerability in Confluence Data Center and Server [1,2].

It is recommended updating affected products as soon as possible.

Technical Details

The vulnerability **CVE-2024-1597**, with a CVSS score of 10.0, is a SQLi (SQL Injection) vulnerability that could allow an unauthenticated attacker to expose assets in the environment [3].

The vulnerability **CVE-2024-21677**, with a CVSS score of 8.3, is a Path Traversal vulnerability that could allow an unauthenticated attacker to exploit an undefinable vulnerability and requires user interaction [4].

The other 22 vulnerabilities have a CVSS score of 7.5 and could lead to DoS conditions, Remote Code Execution, or Server-Side Request Forgery on the affected product.

Affected Products

The vulnerabilities affect the following products:

- Bamboo Data Center and Server;
- Bitbucket Data Center and Server;
- Confluence Data Center and Server;
- Jira Software Data Center and Server.

Please refer to the vendor's advisory [1] for a complete list of affected and fixed versions.

Recommendations

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

References

[1] https://confluence.atlassian.com/security/security-bulletin-march-19-2024-1369444862.html

[2] https://www.atlassian.com/trust/data-protection/vulnerabilities

[3] https://jira.atlassian.com/browse/BAM-25716

[4] https://jira.atlassian.com/browse/CONFSERVER-94604