Security Advisory 2023-068

High Severity Vulnerability in Bitbucket Data Center and Server

September 20, 2023 — v1.0

TLP:CLEAR

History:
- 20/09/2023 — v1.0 – Initial publication

Summary
On September 19, Atlassian released a security bulletin addressing several vulnerabilities among which a high severity vulnerability, identified by CVE-2023-22513, that could allow an authenticated attacker to execute arbitrary code on the server.

It is recommended updating as soon as possible.

Technical Details
The vulnerability CVE-2023-22513, with a CVSS Score of 8.5, could allow an authenticated attacker to execute arbitrary code on the server, which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction.

Affected Products
This vulnerability affects Atlassian Bitbucket Data Center and Server versions 8.0.0, 8.1.0, 8.2.0, 8.3.0, 8.4.0, 8.5.0, 8.6.0, 8.7.0, 8.8.0, 8.9.0, 8.10.0, 8.11.0, 8.12.0, and 8.13.0 [2].

Recommendations
CERT-EU strongly recommends that all installations running a version affected by the issues described above are upgraded to the latest version as soon as possible.

Workaround
When it is not possible to upgrade affected servers to the latest version, it is recommended upgrading them to one of the specified supported fixed versions:
- Bitbucket Data Center and Server 8.9: Upgrade to a release greater than or equal to 8.9.5
- Bitbucket Data Center and Server 8.10: Upgrade to a release greater than or equal to 8.10.5
• Bitbucket Data Center and Server 8.11: Upgrade to a release greater than or equal to 8.11.4
• Bitbucket Data Center and Server 8.12: Upgrade to a release greater than or equal to 8.12.2
• Bitbucket Data Center and Server 8.13: Upgrade to a release greater than or equal to 8.13.1
• Bitbucket Data Center and Server 8.14: Upgrade to a release greater than or equal to 8.14.0
• Bitbucket Data Center and Server version >= 8.0 and < 8.9: Upgrade to any of the listed fix versions.

References