Security Advisory 2022-081

Critical Vulnerabilities in Atlassian Products

November 18, 2022 — v1.0

TLP:CLEAR

History:

- *18/11/2022 — v1.0 – Initial publication*

Summary

On November 16, 2022, Atlassian released two advisories for critical vulnerabilities in the Crowd Server and Data Center identity management platform, and in Bitbucket Server and Data Center. Tracked as `CVE-2022-43782`, the first vulnerability allows an attacker to authenticate as the Crowd application and subsequently call privileged endpoints on the Crowd platform [1]. The second vulnerability, tracked as `CVE-2022-43781`, is a command injection vulnerability in BitBucket that lets an attacker with permission to control their username to exploit this issue and execute arbitrary code on the system [2].

Technical Details

Introduced in Crowd 3.0.0, `CVE-2022-43782` allows an attacker connecting from an IP in the allow list to authenticate as the Crowd application and bypassing a password check. Two conditions need to be met for the vulnerability to be exploited:

- the instance needs to be new installation of version > 3.0.0. Instances being upgrades from earlier versions to the vulnerable version are not affected,
- the IP address has been added to the allow list `Remote Address` of the Crowd application (none by default)

`CVE-2022-43781` might be exploited by unauthenticated users if `Public Signup` is enabled. It does not affect instances running PostgreSQL and those hosted by Atlassian.

Affected Products

The following products are affected [1][2].

- Crowd Server and Data Center for `CVE-2022-43782`:
  - Crowd 3.0.0 to Crowd 3.7.2
  - Crowd 4.0.0 to Crowd 4.4.3
  - Crowd 5.0.0 to Crowd 5.0.2
- Bitbucket Server and Data Center for `CVE-2022-43781`:

- 7.0 to 7.5 (all versions)
- 7.6.0 to 7.6.18
- 7.7 to 7.16 (all versions)
- 7.17.0 to 7.17.11
- 7.18 to 7.20 (all versions)
- 7.21.0 to 7.21.5

If `mesh.enabled=false` is set in `bitbucket.properties`:

- 8.0.0 to 8.0.4
- 8.1.0 to 8.1.4
- 8.2.0 to 8.2.3
- 8.3.0 to 8.3.2
- 8.4.0 to 8.4.1

Recommendations

CERT-EU highly recommends to install the latest fixes of the vendor as specified in the security advisories.

References

[1] https://confluence.atlassian.com/crowd/crowd-security-advisory-november-2022-1168866129.html

[2] https://confluence.atlassian.com/bitbucketserver/bitbucket-server-and-data-center-security-advisory-2022-11-16-1180141667.html