KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Atlassian Patches two Critical Flaws Affecting Crowd and Bitbucket

Tracker ID: TN1119 **Date:** 21/Nov/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Background

Atlassian has recently published November 2022, Atlassian Security Advisories Overview, addressing two critical vulnerabilities reported in Crowd, Bitbucket Server, and Bitbucket Data Center. The vulnerabilities, identified as CVE-2022-43781 and CVE-2022-43782, both received a CVSS vulnerability score of 9.8 out of 10.

CVE-2022-43781 is a command injection vulnerability in Bitbucket Server and Data Center that exploits environment variables. An attacker with permission to control their username can exploit this issue to gain code execution and execute code on the system. It was introduced in Bitbucket Server and Data Center version 7.0.0 and affects versions 7.0 to 7.21 and 8.0 to 8.4. (only if "mesh.enabled" is set to false in "bitbucket.properties"). Also, Bitbucket Server and Data Center instances running PostgreSQL are not affected.

Disabling "Public Signup" is a temporary workaround for CVE-2022-43781. Disabling public signup would shift the attack vector from unauthenticated to authenticated, reducing the likelihood of exploitation. To turn off this feature, navigate to **Administration > Authentication** and uncheck the **Allow public sign up** checkbox. However, when public signup is blocked, ADMIN or SYS ADMIN authenticated users can still exploit the issue.

The second vulnerability, CVE-2022-43782, is induced by a misconfiguration in Crowd Server and Data Center, which allows an attacker to connect from an IP in the allow list and authenticate as the Crowd application by bypassing a password check. This would allow the attacker to utilize the **usermanagement** path to access privileged endpoints in crowd REST API. It can only be exploited by IPs indicated in the Remote Addresses configuration of the crowd application's allowlist.

CVE-2022-43782 was discovered during an internal security evaluation of Crowd 3.0.0, affects all new installations; thus, users who upgraded from Crowd 3.0.0 are not at risk. For example, upgrading from version 2.9.1 to 3.0.0 has no effect on your instance. However, any default remote addresses from version 2.9.1 will be passed over to the instance running version 3.0.0 in this situation. These can also be removed from the crowd application's remote address setup.

It is not unusual for vulnerabilities in Atlassian and Bitbucket to be actively exploited in the wild, making it critical that users implement patches as soon as possible. The US Cybersecurity and Infrastructure Security Agency (CISA) notified last month that a command injection issue in Bitbucket Server and Data Center (CVE-2022-36804, CVSS score: 9.9) had been leveraged in attacks since late September 2022.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG Cyber Threat Intelligence Platform

Cyber Threat Notification | Atlassian Patches two Critical Flaws Affecting Crowd and Bitbucket

Tracker ID: TN1119 **Date:** 21/Nov/2022 **Category:** Vulnerability **Industry:** All **Region**: All

Analysis

CVE ID	Severity	CVSS Score
CVE-2022-43781	Critical	9.8
CVE-2022-43782	Critical	9.8

Affected Products and Versions

The following supported versions products are affected:

- Bitbucket Server and Data Center:
    - 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) and 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 and 8.4.0 to 8.4.1
- Crowd released after 3.0.0 are affected. All the new installations running any of the following versions: Crowd 3.0.0 - Crowd 3.7.2, Crowd 4.0.0 - Crowd 4.4.3 and Crowd 5.0.0 - Crowd 5.0.2.

Recommendations

- Affected customers are recommended to install the relevant updated versions of Atlassian Crowd, Bitbucket Server, and Bitbucket Data Center as soon as possible.
- For Bitbucket Server and Data Center products, upgrade to 7.6.19 or newer; 7.17.12 or newer; 7.21.6 or newer; 8.0.5 or newer; 8.1.5 or newer; 8.2.4 or newer; 8.3.3 or newer; 8.4.2 or newer and 8.5.0 or newer.
- For Crowd 5.0 upgrade to 5.0.3 or later; For Crowd 4.0 upgrade to 4.4.4 or later. Crowd 3.0 version has been deprecated, there's no fix available. Thus, please upgrade to Crowd 4.4.4 or 5.0.3.

References

- Atlassian Support, November 2022: Atlassian Security Advisories Overview, Atlassian, 16th November 2022, External Link (confluence.atlassian.com).
- Bitbucket Support, Bitbucket Server and Data Center Security Advisory 2022-11-16, Atlassian, 16th November 2022, External Link (confluence.atlassian.com).
- Crowd Support, Crowd Security Advisory (November 2022), Atlassian, 16th November 2022, External Link (confluence.atlassian.com).

In case of a Security Incident, please report to IN-FM KPMG SOC.

For any query or feedback, feel free to reach us at IN-FM KPMG CTI.

KPMG in India Cyber Response Hotline : +91 9176471471