CERT-EU

Security Advisory 2023-085

Critical Vulnerability in Confluence Data Center and Server

November 8, 2023 — v1.2

TLP:CLEAR

History:

- *31/10/2023 — v1.0 – Initial publication*
- *03/11/2023 — v1.1 – Information about public exploit and mitigation measures*
- *08/11/2023 — v1.2 – Change of the impact of the vulnerability*

Summary

On October 30 2023, a notable vulnerability, **CVE-2023-22518**, affecting Confluence Data Center and Server was disclosed by Atlassian [1]. The exploitation of this vulnerability could result in significant data loss. Updates are already available for this vulnerability. The CVE-2023-22518 had an initial CVSS score of 9.1 indicating a critical risk.

On November 2, Atlassian warned that the risk of exploitation increased as critical information about the vulnerability has been publicly exposed [1]. While there is no report of active exploitation, it is highly recommended updating affected products as soon as possible.

[Update] On November 6, Atlassian has escalated **CVE-2023-22518** CVSS score from 9.1 to 10, the highest critical rating, due to the change in the scope of the attack.

Technical Details

[Update] The vulnerability `CVE-2023-22518` is an Improper Authorization checks vulnerability that allows an unauthenticated attacker to reset Confluence and create a Confluence instance administrator account. Using this account, an attacker can then perform all administrative actions that are available to Confluence instance administrator leading to - but not limited to - full loss of confidentiality, integrity and availability.

Threat Detections

[Update] Evidence of compromise may include:

- loss of login access to the instance
- requests to `/json/setup-restore*` in network access logs
- installed unknown plugins
- encrypted files or corrupted data
- unexpected members of the `confluence-administrators` group
- unexpected newly created user accounts

If any evidence is found, you should assume that the instance has been compromised.

Affected Products

The flaw impacts all Confluence Data Center and Server versions:

- before 7.19.16;
- before 8.3.4;
- before 8.4.4;
- before 8.5.3;
- before 8.6.1.

Versions outside of the support window (i.e., versions that have reached end-of-life) may also be affected, so Atlassian recommends you upgrade to a fixed LTS version or later.

Recommendations

CERT-EU recommends updating to a fixed version as soon as possible.

Mitigations

In case the patch cannot be applied, CERT-EU and Atlassian recommend removing the instance from the internet until the patch is deployed, if possible. Instances accessible to the public internet, including those with user authentication, should be restricted from external network access. It is also recommended to back up Confluence Data Center and Server instances if not done already.

Furthermore, if removing the instance from the internet is not possible, it is possible to remove known attack vectors by blocking access on the following endpoints by modifying the `/<confluence-install-dir>/confluence/WEB-INF/web.xml`, and restarting the vulnerable instances:

- `/json/setup-restore.action`;
- `/json/setup-restore-local.action`;
- `/json/setup-restore-progress.action`.

These mitigation actions are limited and **are not a replacement for patching**!

References

[1] https://confluence.atlassian.com/security/cve-2023-22518-improper-authorization-vulnerability-in-confluence-data-center-and-server-1311473907.html

[2] https://www.bleepingcomputer.com/news/security/atlassian-warns-of-exploit-for-confluence-data-wiping-bug-get-patching/