CERT-EU

Security Advisory 2023-073

Access Control Vulnerability in Confluence Data Center and Server

October 6, 2023 — v1.0

TLP:CLEAR

History:

- *6/10/2023 — v1.0 – Initial publication*

Summary

Atlassian has been made aware of a critical vulnerability, CVE-2023-22515, a Broken Access Control vulnerability in Confluence Data Center and Server. External attackers may exploit this vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorised Confluence administrator accounts and access Confluence instances. Atlassian Cloud sites are **not affected** by this vulnerability.

Technical Details

External attackers can exploit a vulnerability in publicly accessible Confluence Data Center and Server instances. This allows them to create unauthorized Confluence administrator accounts and access the said instances. The vulnerability seems to impact the `/setup/*.action` and `/server-info.action` endpoints but no further technical details are provided yet.

Affected Products

Confluence Data Center and Server versions:

- 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 8.4.2
- 8.5.0 to 8.5.1

Note: Versions prior to 8.0.0 are **not affected**.

Detections

Even after an updating Confluence to a fixed version, ensure you check all affected Confluence instances for:

1. Unexpected members of the `confluence-administrators` group.
2. Newly created user accounts that were not expected.
3. Requests to `/setup/*.action` in network access logs.
4. Presence of `/setup/setupadministrator.action` in an exception message in the Confluence home directory (`atlassian-confluence-security.log`)
5. Presence of `/server-info.action` in network access logs, as mentionned by Rapid7 [2].

Recommendations

It is recommended to upgrade to one of the following fixed versions (or any later version):

- 8.3.3 or later
- 8.4.3 or later
- 8.5.2 (Long Term Support release) or later

If upgrading is not immediately possible, you should:

1. Restrict external network access to the affected instance.
2. Block access to the `/setup/*` endpoints. This can be done at the network layer or by modifying configuration files as described:
    - On each node, modify `/<confluence-install-dir>/confluence/WEB-INF/web.xml` to include:

```
<security-constraint>
      <web-resource-collection>
        <url-pattern>/setup/*</url-pattern>
   <http-method-omission>*</http-method-omission>
  </web-resource-collection>
      <auth-constraint />
 </security-constraint>
```

    - Restart Confluence.

References

[1] https://confluence.atlassian.com/security/cve-2023-22515-privilege-escalation-vulnerability-in-confluence-data-center-and-server-1295682276.html

[2] https://www.rapid7.com/blog/post/2023/10/04/etr-cve-2023-22515-zero-day-privilege-escalation-in-confluence-server-and-data-center/