Security Advisory 2022-031

Jira Authentication Bypass Vulnerability

April 26, 2022 — v1.0

TLP:WHITE

History:

- *26/04/2022 — v1.0 – Initial publication*

Summary

On April 20th, Atlassian published a security advisory for a critical vulnerability in the Jira and Jira Service Management products, that are vulnerable to an authentication bypass in its web authentication framework, Jira Seraph. This vulnerability is tracked as **CVE-2022-0540**, with a severity score of 9.9 out of 10 on the CVSS scoring system. Atlassian has released software updates that address this vulnerability [1].

Technical Details

CVE-2022-0540 (CVSS: Critical 9.9)

A remote, unauthenticated attacker could exploit this vulnerability by sending a specially crafted HTTP request to bypass authentication and authorization requirements in WebWork actions using an affected configuration.

Atlassian specifies that remote attackers can only compromise the impacted products if they use a specific configuration in Seraph, which is described as follows:

"Although the vulnerability is in the core of Jira, it affects first and third party apps that specify roles-required at the webwork1 action namespace level and do not specify it at an action level. For a specific action to be affected, the action will also need to not perform any other authentication or authorization checks."

For an app to be affected by CVE-2022-0540, both of the following conditions must be true:

- it is installed in one of the affected Jira or Jira Service Management versions listed below,
- it is using a configuration vulnerable to CVE-2022-0540.

Products Affected

Affected Jira Versions

This includes **Jira Core Server**, **Jira Software Server** and **Jira Software Data Center**

- All versions before 8.13.18
- 8.14.x
- 8.15.x
- 8.16.x
- 8.17.x
- 8.18.x
- 8.19.x
- 8.20.x before 8.20.6
- 8.21.x

Affected Jira Service Management Versions

This includes **Jira Service Management Server** and **Jira Service Management Data Center**

- All versions before 4.13.18
- 4.14.x
- 4.15.x
- 4.16.x
- 4.17.x
- 4.18.x
- 4.19.x
- 4.20.x before 4.20.6
- 4.21.x

Recommendations

Atlassian recommends installing a fixed version of Jira or Jira Service Management to remediate CVE-2022-0540.

Fixed Jira Versions:

- 8.13.x >= 8.13.18
- 8.20.x >= 8.20.6
- All versions >= 8.22.0

Fixed Jira Service Management Versions

- 4.13.x >= 4.13.18
- 4.20.x >= 4.20.6
- All versions >= 4.22.0

Workarounds

If it is not possible to update to one of the versions above and you are using any affected apps, Atlassian recommends updating the affected apps to a version that has remediated the risk, or disabling the vulnerable apps until patching is possible.

References

[1] https://confluence.atlassian.com/jira/jira-security-advisory-2022-04-20-1115127899.html