Hive Pro

THREAT ADVISORY

Bypass Authentication vulnerability in Atlassian Jira Seraph

TA2022099

Threat Level GREEN

Publish Date – April 25, 2022

Atlassian has addressed a vulnerability in its Jira Seraph software, tracked as CVE-2022-0540. An unauthenticated attacker can use to bypass authentication. By submitting a specially crafted HTTP request to affected software, a threat actor could exploit the vulnerability. Although the vulnerability exists in Jira's core, it only affects first and third-party apps that define roles-required at the webwork1 action namespace level rather than at the action level. For a given operation to be affected, it must also not complete any further authentication or authorization checks.

This vulnerability has been fixed in Atlassian Jira Server & Data Center versions 8.13.18, 8.20.6 and 8.22.0 and Atlassian Jira Service Management Server and Data Center versions 4.13.18, 4.20.6 and 4.22.0

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-0540	Atlassian Jira Server and Data Center versions before 8.13.18, versions 8.14.0 to 8.20.6, and versions 8.21.0 to 8.22.0; Atlassian Jira Service Management Server and Data Center versions before 4.13.18, versions 4.14.0 to 4.20.6, and versions 4.21.0 to 4.22.0	cpe:2.3:a:atlassian:jira:*:*:*:*:server:*:*:*, cpe:2.3:a:atlassian:jira:*:*:*:*:data_center:*:*:* , cpe:2.3:a:atlassian:jira_service_management:*:*:*:*:server:*:*:* , cpe:2.3:a:atlassian:jira_service_management:*:*:*:*:data_center:*:*:*	Atlassian Jira server/data center seraph improper authentication vulnerability	CWE-287

Patch Links

https://www.atlassian.com/software/jira/core/download
https://www.atlassian.com/software/jira/update

References

https://confluence.atlassian.com/jira/jira-security-advisory-2022-04-20-1115127899.html
https://jira.atlassian.com/browse/JSDSERVER-11224
https://jira.atlassian.com/browse/JRASERVER-73650