October 19, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The vulnerabilities reported in this security bulletin include 2 critical and 26 high-severity vulnerabilities which have been fixed in new versions of our products, released in the last month. These vulnerabilities are discovered via our Bug Bounty program and pen-testing processes, as well as third party library scans.

Technical Details

Released Security Vulnerabilities			
Summary	**Severity**	**CVSS Score**	**Affected Versions**
Broken Access Control Vulnerability in Confluence Data Center and Server	**Critical**	10.0	All versions of Confluence Data Center and Server including and after 8.0.0
XXE (XML External Entity Injection) in Jira Service Management Data Center and Server	**Critical**	9.8	All versions of Jira Service Management Data Center and Server including and after 4.20.0
RCE (Remote Code Execution) in Sourcetree for Mac and Windows	**High**	7.8	All Windows versions including and after 3.4.0 All Mac versions including and after 4.1.0
com.google.protobuf:protobuf-java Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
com.google.protobuf:protobuf-java Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
com.google.protobuf:protobuf-java Vulnerability in Jira Service Management Data Center and Server	**High**	5.5	All versions including and after 4.20.0
FasterXML Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
FasterXML Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
jackson-databind Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
jackson-databind Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
Json-smart Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
Json-smart Vulnerability in Jira Service Management Data Center and Server	**High**	7.5	All versions including and after 4.20.0
Apache Kafka Connect API Vulnerability in Bitbucket Data Center and Server	**High**	8.8	All versions including and after 7.21.0
FasterXML Vulnerability in Bitbucket Data Center and Server	**High**	7.5	All versions including and after 7.17.0
FasterXML Vulnerability in Bitbucket Data Center and Server	**High**	7.5	All versions including and after 7.17.0
jackson-databind Vulnerability in Bitbucket Data Center and Server	**High**	7.5	All versions including and after 7.17.0

jackson-databind Vulnerability in Bitbucket Data Center and Server	**High**	7.5	All versions including and after 7.17.0
com.google.code.gson Vulnerability in Bitbucket Data Center and Server	**High**	7.5	All versions including and after 7.17.0
Jettison Vulnerability in Bitbucket Data Center and Server	**High**	7.5	All versions including and after 7.17.0
hutool-json Vulnerability in Bitbucket Data Center and Server	**High**	7.5	All versions including and after 7.17.0
Woodstox Vulnerability in Bamboo Data Center and Server	**High**	7.5	All versions including and after 9.1.0
FasterXML Vulnerability in Bamboo Data Center and Server	**High**	7.5	All versions including and after 9.1.0
FasterXML Vulnerability in Bamboo Data Center and Server	**High**	7.5	All versions including and after 9.1.0
jackson-databind Vulnerability in Bamboo Data Center and Server	**High**	7.5	All versions including and after 9.1.0
jackson-databind Vulnerability in Bamboo Data Center and Server	**High**	7.5	All versions including and after 9.1.0
org.apache.tomcat:tomcat-catalina Vulnerability in Bamboo Data Center and Server	**High**	7.5	All versions including and after 9.2.2

This vulnerability is rated as a **CRITICAL**. A software update exists to address this risk.

To fix all the vulnerabilities in this bulletin, Atlassian recommends upgrading your instances to the latest version, if you're unable to do so, upgrade to the minimum fix version in the table below.

Product	Fix Recommendation
Confluence Server and Data Center	Upgrade to a minimum fix version of 8.3.3, 8.4.3, 8.5.2 or latest
Jira Service Management Data Center and Server	Upgrade to a minimum fix version of 4.20.27, 5.4.11 or latest
Bitbucket Data Center and Server	Upgrade to a minimum fix version of 7.21.16, 8.9.4, 8.11.3,8.12.1, 8.13.1 or latest
Bamboo Data Center and Server	Upgrade to a minimum fix version of 9.2.5, 9.3.1, 9.3.3 or latest
Sourcetree for Windows	Upgrade to a minimum fix version of 3.4.15 or latest
Sourcetree for Mac	Upgrade to minimum fix version of 4.2.5 or latest

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-22515, CVE-2019-13990, CVE-2023-22514, CVE-2022-3509, CVE-2022-3171, CVE-2021-22569, CVE-2022-42004, CVE-2022-42003, CVE-2021-46877, CVE-2020-36518, CVE-2021-31684, CVE-2023-1370, CVE-2023-25194, CVE-2022-42004, CVE-2022-42003, CVE-2021-46877, CVE-2020-36518, CVE-2022-45685, CVE-2022-45688, CVE-2022-40152, CVE-2022-42004, CVE-2022-42003, CVE-2021-46877, CVE-2020-36518, CVE-2023-28709
- Security Bulletin - October 17 2023

Please note that we will be transitioning to a new site on August 31, 2023, where we will post the vulnerability reports.

You will be able to find all the reports that we have published as well as all future reports here: Cybersecurity Alerts