December 1, 2023

Overall rating: High

BRITISH COLUMBIA

This is a technical bulletin intended for technical audiences.

Summary

Atlassian has published a security bulletin to address vulnerabilities in the following products: Bamboo data center and server – version 8.1.0 and later, Bitbucket data center and server – version 7.21.0 and later, Confluence data center and server – version 6.13.0 and later, Crowd data center and server – version 3.4.6 and later, and Jira software data center and server – version 8.20.0 and later.

The vulnerabilities reported in this security bulletin include 26 high-severity vulnerabilities which have been fixed in new versions of Atlassian products, released in the last month.

Technical Details

Summary	Severity	CVSS Score	Affected Versions	CVE ID	A
Info Disclosure com.google.guava:guava in Jira Software Data Center and Server	High	7.1	All versions including and after 8.20.0	CVE-2023-2976	J
DoS (Denial of Service) com.google.code.gson:gson in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2022-25647	J
DoS (Denial of Service) org.jsoup:jsoup in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2021-37714	J
Deserialization com.fasterxml.jackson.core:jackson-databind in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2022-42004	J
DoS (Denial of Service) com.fasterxml.jackson.core:jackson-databind in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2022-42003	J
DoS (Denial of Service) jackson-databind in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2021-46877	J
DoS (Denial of Service) com.fasterxml.jackson.core in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2020-36518	J
DoS (Denial of Service) org.apache.tomcat:tomcat-catalina in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2023-42794	J
DoS (Denial of Service) io.netty:netty-codec-http2 in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2023-44487	J
Cache Poisoning org.eclipse.jetty:jetty-server in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2017-7656	J
DoS (Denial of Service) org.eclipse.jetty:jetty-io in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2021-28165	J
Info Disclosure org.eclipse.jetty:jetty-util in Jira Software Data Center and Server	High	7.5	All versions including and after 8.20.0	CVE-2017-9735	J
RCE (Remote Code Execution) in Crowd Data Center and Server	High	8	All versions including and after 3.4.6	CVE-2023-22521	C
SSRF org.apache.xmlgraphics in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2022-41704	C

SSRF org.apache.xmlgraphics:batik-bridge in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2022-40146
XSS org.apache.xmlgraphics:batik-script in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2022-42890
org.apache.tomcat:tomcat-catalina Vulnerability in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2022-45143
DoS (Denial of Service) net.sourceforge.nekohtml:nekohtml in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2022-28366
Request Smuggling org.apache.tomcat:tomcat-coyote in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2022-42252
DoS (Denial of Service) org.apache.tomcat:tomcat-catalina in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2023-42794
DoS (Denial of Service) io.netty:netty-codec-http2 in Confluence Data Center and Server	High	7.5	All versions including and after 6.13.0	CVE-2023-44487
Third-Party Dependency in Bitbucket Data Center and Server	High	7.5	All versions including and after 7.21.0	CVE-2021-40690
DoS (Denial of Service) apache-struts in Bamboo Data Center and Server	High	7.5	All versions including and after 8.1.0	CVE-2023-34396
DoS (Denial of Service) org.apache.tomcat:tomcat-catalina in Bamboo Data Center and Server	High	7.5	All versions including and after 8.1.0	CVE-2023-42794
DoS (Denial of Service) org.apache.tomcat:tomcat-coyote in Bamboo Data Center and Server	High	7.5	All versions including and after 8.1.0	CVE-2023-44487
RCE (Remote Code Execution) in Bamboo Data Center and Server	High	8.5	All versions including and after 8.1.0	CVE-2023-22516

A software version updates exists to address these risks.

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

- Atlassian Security Bulletin - November 21 2023
- VRM Vulnerability Reports