مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates-Multiple Vulnerabilities Atlassian Products

Tracking #:432315716

Date:20-03-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Atlassian recently released security updates to address multiple vulnerabilities in its products.

TECHNICAL DETAILS:

Atlassian released security updates to address multiple vulnerabilities in several of its products, including Bamboo, Bitbucket, Confluence, and Jira Software. These vulnerabilities include SQL Injection (SQLi), Denial-of-Service (DoS), Path Traversal, Remote Code Execution (RCE), and Server-Side Request Forgery (SSRF). They could be exploited by an attacker to compromise affected systems.

Vulnerabilities Details:

Description	CVE	Severity
SQLi (SQL Injection) org.postgresql:postgresql Dependency in Bamboo Data Center and Server	CVE-2024-1597	10.0 **Critical**
DoS (Denial of Service) software.amazon.ion:ion-java Dependency in Bamboo Data Center and Server	CVE-2024-21634	7.5 High
DoS (Denial of Service) software.amazon.ion:ion-java Dependency in Bitbucket Data Center and Server	CVE-2024-21634	7.5 High
Path Traversal in Confluence Data Center	CVE-2024-21677	8.3 High
DoS (Denial of Service) org.eclipse.jetty:jetty-http Dependency in Confluence Data Center and Server	CVE-2023-36478	7.5 High
DoS (Denial of Service) org.codehaus.jettison:jettison Dependency in Jira Software Data Center and Server	CVE-2022-40150	7.5 High
DoS (Denial of Service) org.xerial.snappy:snappy-java Dependency in Jira Software Data Center and Server	CVE-2023-34455	7.5 High
RCE (Remote Code Execution) org.apache.xmlgraphics:batik-script Dependency in Jira Software Data Center and Server	CVE-2022-42890	7.5 High
RCE (Remote Code Execution) org.apache.xmlgraphics:batik-bridge Dependency in Jira Software Data Center and Server	CVE-2022-41704	7.5 High
SSRF (Server-Side Request Forgery) org.apache.xmlgraphics:batik-bridge Dependency in Jira Software Data Center and Server	CVE-2022-40146	7.5 High
DoS (Denial of Service) org.codehaus.jettison:jettison	CVE-2023-1436	7.5 High

Dependency in Jira Software Data Center and Server		
DoS (Denial of Service) org.codehaus.jettison:jettison Dependency in Jira Software Data Center and Server	CVE-2022-45685	7.5 High
DoS (Denial of Service) net.sourceforge.nekohtml:nekohtml Dependency in Jira Software Data Center and Server	CVE-2022-29546	7.5 High
DoS (Denial of Service) org.codehaus.jettison:jettison Dependency in Jira Software Data Center and Server	CVE-2022-40149	7.5 High
DoS (Denial of Service) org.apache.avro:avro Dependency in Jira Software Data Center and Server	CVE-2023-39410	7.5 High
DoS (Denial of Service) org.xerial.snappy:snappy-java Dependency in Jira Software Data Center and Server	CVE-2023-34454	7.5 High
DoS (Denial of Service) org.xerial.snappy:snappy-java Dependency in Jira Software Data Center and Server	CVE-2023-34453	7.5 High
DoS (Denial of Service) org.xerial.snappy:snappy-java Dependency in Jira Software Data Center and Server	CVE-2023-43642	7.5 High
DoS (Denial of Service) com.google.protobuf:protobuf-java Dependency in Jira Software Data Center and Server	CVE-2022-3509	7.5 High
DoS (Denial of Service) com.google.protobuf:protobuf-java Dependency in Jira Software Data Center and Server	CVE-2022-3171	7.5 High
DoS (Denial of Service) org.json:json Dependency in Jira Software Data Center and Server	CVE-2023-5072	7.5 High
DoS (Denial of Service) org.json:json Dependency in Jira Software Data Center and Server	CVE-2022-45688	7.5 High
RCE (Remote Code Execution) xalan:xalan Dependency in Jira Software Data Center and Server	CVE-2022-34169	7.5 High
DoS (Denial of Service) net.sourceforge.nekohtml:nekohtml Dependency in Jira Software Data Center and Server	CVE-2022-24839	7.5 High
DoS (Denial of Service) net.sourceforge.nekohtml:nekohtml Dependency in Jira Software Data Center and Server	CVE-2022-28366	7.5 High

Fixed Versions:

Bamboo Data Center and Server

- 9.6.0 (LTS) or 9.5.2 recommended Data Center Only

- 9.4.4
- 9.2.12 (LTS)

Bitbucket Data Center and Server

- 8.19.0 (LTS) recommended Data Center Only
- 8.18.1
- 8.17.2
- 8.16.3 to 8.16.4
- 8.15.4 to 8.15.5
- 8.14.5 to 8.14.6
- 8.13.6
- 8.9.10 to 8.9.11 (LTS)
- 7.21.22 to 7.21.23

Confluence Data Center and Server

- 8.8.1 recommended Data Center Only
- 8.5.7 (LTS)
- 7.19.20 (LTS)

Jira Software Data Center and Server

- 9.14.1 recommended or 9.14.0 Data Center Only
- 9.13.0 to 9.13.1
- 9.12.3 to 9.12.5 (LTS)
- 9.4.18 (LTS)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Atlassian.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

https://confluence.atlassian.com/security/security-bulletin-march-19-2024-1369444862.html