مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Security Updates – Atlassian Products

Tracking #:432316169

Date:21-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Atlassian released security updates to address multiple high severity vulnerabilities in their products.

TECHNICAL DETAILS:

Atlassian released security updates to address 9 high-severity vulnerabilities for various products, including Bamboo, Confluence, Jira and Crowd Data Center and Server.

1) **Bamboo Data Center and Server**

- **CVE-2024-21689:** RCE (Remote Code Execution) in Bamboo Data Center and Server (CVSS: 7.6 High)
- **CVE-2024-29857**: DoS (Denial of Service) org.bouncycastle:bcprov-jdk18on Dependency in Bamboo Data Center and Server (CVSS: 7.5 High)
- **Affected Versions:**
  - 9.6.0 to 9.6.4 (LTS)
  - 9.5.0 to 9.5.3
  - 9.4.0 to 9.4.4
  - 9.3.0 to 9.3.6
  - 9.2.1 to 9.2.16 (LTS)
  - 9.1.0 to 9.1.3
  - 9.0.0 to 9.0.4
- **Fixed Versions:**
  - 9.6.5 (LTS) recommended Data Center Only
  - 9.2.17 (LTS)

2) **Confluence Data Center and Server**

- **CVE-2024-34750-**DoS (Denial of Service) org.apache.tomcat:tomcat-coyote Dependency in Confluence Data Center and Server: Stored XSS (CVSS: 7.5 High)
- **CVE-2024-21690**-Reflected XSS and CSRF (Cross-Site Request Forgery) in Confluence Data Center and Server-(CVSS: 7.1 High)
- **Affected Versions:**
  - 8.9.0 to 8.9.5
  - 8.8.0 to 8.8.1
  - 8.7.1 to 8.7.2
  - 8.6.0 to 8.6.2
  - 8.5.0 to 8.5.12 (LTS)
  - 8.4.0 to 8.4.5
  - 8.3.0 to 8.3.4
  - 8.2.0 to 8.2.3
  - 8.1.0 to 8.1.4
  - 8.0.0 to 8.0.4
  - 7.20.0 to 7.20.3

- **Fixed Versions:**
  - 9.0.1 to 9.0.2 Data Center Only
  - 8.5.14 (LTS) recommended
  - 7.19.26 (LTS)

3) **Crowd Data Center and Server**

- **CVE-2024-22259, CVE-2024-22243,CVE-2024-22262**: SSRF (Server-Side Request Forgery) org.springframework:spring-web Dependency in Crowd Data Center and Server (CVSS: 8.1 High)
- **Affected Versions**:
  - 5.3.0 to 5.3.2
  - 5.2.0 to 5.2.4
  - 5.1.0 to 5.1.9
- **Fixed Versions**:
  - 6.0.0 to 6.0.1 Data Center Only
  - 5.3.3 recommended
  - 5.2.6 to 5.2.7
  - 5.1.11

4) **Jira Service Management Data Center and Server**

- **CVE-2024-34750-**DoS (Denial of Service) org.apache.tomcat:tomcat-coyote Dependency in Jira Software Data Center and Server (CVSS: 7.5 High)
- **Affected Versions:**
  - 5.17.0
  - 5.16.0 to 5.16.1
  - 5.12.0 to 5.12.11 (LTS)
  - 5.4.0 to 5.4.24 (LTS)
- **Fixed Versions**:
  - 5.17.1 to 5.17.2 Data Center Only
  - 5.12.12 (LTS) recommended
  - 5.4.25 (LTS)

5) **Jira Data Center and Server**

- **CVE-2024-34750-**DoS (Denial of Service) org.apache.tomcat:tomcat-coyote Dependency in Jira Software Data Center and Server (CVSS: 7.5 High)
- **Affected Versions:**
  - 9.17.0
  - 9.16.0 to 9.16.1
  - 9.12.0 to 9.12.11 (LTS)
  - 9.4.0 to 9.4.24 (LTS)

- **Fixed Versions**:
  - 9.17.1 to 9.17.2 Data Center Only
  - 9.12.12 (LTS) recommended
  - 9.4.25 (LTS)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install the relevant security updates 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-august-20-2024-1431535667.htmll