



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Atlassian Security Updates

Tracking #:432315965

Date:20-06-2024

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

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

TECHNICAL DETAILS:

Atlassian has addressed high severity vulnerabilities in Confluence, Crucible, Jira Core, and Jira Service Management. These vulnerabilities could be exploited by attackers to gain unauthorized access to systems, execute arbitrary code, or crash applications.

Vulnerabilities Details:

CVE ID	CVSS Severity	Description
CVE-2024-22257	8.2 High	Improper Authorization org.springframework.security:spring-security-core Dependency in Confluence Data Center and Server
CVE-2024-22243	8.1 High	SSRF (Server-Side Request Forgery) org.springframework:spring-web Dependency in Confluence Data Center and Server
CVE-2024-22262	8.1 High	SSRF (Server-Side Request Forgery) org.springframework:spring-web Dependency in Confluence Data Center and Server
CVE-2024-22259	8.1 High	SSRF (Server-Side Request Forgery) org.springframework:spring-web Dependency in Confluence Data Center and Server
CVE-2024-29133	7.5 High	DoS (Denial of Service) org.apache.commons:commons-configuration2 Dependency in Confluence Data Center and Server
CVE-2024-29131	7.5 High	DoS (Denial of Service) org.apache.commons:commons-configuration2 Dependency in Confluence Data Center and Server
CVE-2022-25647	7.5 High	DoS (Denial of Service) com.google.code.gson:gson Dependency in Crucible Data Center and Server
CVE-2024-21685	7.4 High	Information Disclosure in Jira Core Data Center
CVE-2024-21685	7.4 High	Information Disclosure in Jira Service Management Data Center and Server

Fixed Versions:

- **Confluence Data Center and Server**
 - 8.9.3 Data Center Only
 - 8.5.11 (LTS) recommended
 - 7.19.24 (LTS)
- **Fisheye/Crucible**
 - 4.8.15 recommended
- **Jira Data Center and Server**
 - 9.16.0 to 9.16.1 Data Center Only
 - 9.12.8 to 9.12.10 (LTS) recommended
 - 9.4.21 to 9.4.23 (LTS)
- **Jira Service Management Data Center and Server**
 - 5.16.0 to 5.16.1 Data Center Only
 - 5.12.8 to 5.12.10 (LTS) recommended
 - 5.4.21 to 5.4.23 (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-june-18-2024-1409286211.html>