مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Security Updates- Atlassian
Tracking #:432317848
Date:23-10-2025

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Atlassian has released its October 2025 Security Bulletin, disclosing 14 high-severity vulnerabilities across multiple products, including Jira Software, Jira Service Management, Bamboo, and Fisheye/Crucible.

TECHNICAL DETAILS:

Atlassian has released its October 2025 Security Bulletin, disclosing 14 high-severity vulnerabilities across multiple products, including Jira Software, Jira Service Management, Bamboo, and Fisheye/Crucible.

The flaws include Path Traversal (Arbitrary File Write), Denial-of-Service (DoS) conditions in dependencies such as Tomcat and Netty, SMTP Injection, and HTTP Request Smuggling vulnerabilities.

Successful exploitation could lead to arbitrary file write, service disruption, or unauthorized email injection, potentially compromising system integrity and availability.

Atlassian strongly recommends upgrading to the latest fixed versions immediately to mitigate these vulnerabilities.

Affected Products and Vulnerability Overview:

Product & Release Notes	Affected Versions	Fixed Version	Vulnerability Summary	CVE ID	CVSS Severity
Bamboo Data Center and Server	11.0.0 to 11.0.4 10.2.0 to 10.2.7 (LTS) 9.6.0 to 9.6.16 (LTS)	11.0.5 to 11.0.7 Data Center Only 10.2.8 to 10.2.9 (LTS) recommended Data Center Only 9.6.17 to 9.6.18 (LTS) Data Center Only	DoS (Denial of Service) org.apache.tomcat:tomcat-coyote Dependency in Bamboo Data Center and Server	CVE-2025-48989	7.5 High
Fisheye/Crucible	4.9.0 to 4.9.2 4.8.14 to 4.8.16	4.9.3 to 4.9.4 recommended	DoS (Denial of Service) commons-fileupload:commons-fileupload Dependency in Crucible Data Center and Server	CVE-2025-48976	7.5 High
Jira Data Center and Server	11.0.0 to 11.0.1 10.7.1 to 10.7.4 10.6.0 to 10.6.1 10.5.0 to 10.5.1 10.4.0 to 10.4.1 10.3.0 to 10.3.11	11.1.0 to 11.1.1 Data Center Only 10.3.12 (LTS) recommended Data Center Only 9.12.28 (LTS)	Path Traversal (Arbitrary Write) in Jira Software Data Center and Server	CVE-2025-22167	8.7 High

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

	(LTS) 10.2.0 to 10.2.1 10.1.1 to 10.1.2 10.0.0 to 10.0.1 9.17.0 to 9.17.5 9.16.0 to 9.16.1 9.15.2 9.14.0 to 9.14.1 9.13.0 to 9.13.1 9.12.0 to 9.12.27 (LTS)	recommended	DoS (Denial of Service) io.netty:netty-codec-http Dependency in Jira Software Data Center	CVE-2025-58057	8.7 High
			HTTP Request Smuggling io.netty:netty-codec-http Dependency in Jira Software Data Center	CVE-2025-58056	8.7 High
			DoS (Denial of Service) org.apache.tomcat:tomcat-coyote Dependency in Jira Software Data Center and Server	CVE-2025-48989	7.5 High
			SMTP Injection org.eclipse.angus:angus-mail/org.eclipse.angus:smtp Dependency in Jira Software Data Center	CVE-2025-7962	7.5 High
			SMTP Injection com.sun.mail:jakarta.mail Dependency in Jira Software Data Center	CVE-2025-7962	7.5 High
Jira Service Management Data Center and Server	11.0.0 to 11.0.1 10.7.1 to 10.7.4 10.6.0 to 10.6.1 10.5.0 to 10.5.1 10.4.0 to 10.4.1 10.3.0 to 10.3.11 (LTS) 10.2.0 to 10.2.1 10.1.1 to 10.1.2 10.0.0 to 10.0.1 5.17.0 to 5.17.5 5.16.0 to 5.16.1 5.15.2 5.14.0 to 5.14.1 5.13.0 to 5.13.1 5.12.0 to 5.12.27 (LTS)	11.1.0 to 11.1.1 Data Center Only 10.3.12 (LTS) recommended Data Center Only 5.12.28 (LTS)	Path Traversal (Arbitrary Write) in Jira Service Management Data Center and Server Data Center and Server	CVE-2025-22167	8.7 High
			DoS (Denial of Service) io.netty:netty-codec-http Dependency in Jira Service Management Data Center	CVE-2025-58057	8.7 High

TLP: WHITE

			HTTP Request Smuggling io.netty:netty-codec-http Dependency in Jira Service Management Data Center	CVE-2025-58056	8.7 High
			DoS (Denial of Service) org.apache.tomcat:tomcat-coyote Dependency in Jira Service Management Data Center and Server	CVE-2025-48989	7.5 High
			SMTP Injection com.sun.mail:jakarta.mail Dependency in Jira Service Management Data Center	CVE-2025-7962	7.5 High
			SMTP Injection org.eclipse.angus:angus-mail/org.eclipse.angus:smtp Dependency in Jira Service Management Data Center	CVE-2025-7962	7.5 High

RECOMMENDATIONS:

Apply Security Patches Immediately: Upgrade to the latest fixed versions listed above.

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-october-21-2025-1652920034.html