مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Security Updates – Jenkins

Tracking #:432317724

Date:18-09-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Jenkins has released patches addressing multiple security vulnerabilities affecting both its weekly and Long-Term Support (LTS) releases.

TECHNICAL DETAILS:

Jenkins, a widely deployed open-source automation server, has released patches addressing multiple vulnerabilities impacting both its weekly and Long-Term Support (LTS) releases. These flaws include a denial-of-service weakness in the Jetty server component, missing permission checks leading to unauthorized information disclosure, and log message injection risks. Exploitation of these issues could result in service outages, unauthorized exposure of sensitive configurations, and tampered logs that could hinder incident investigations.

Vulnerability Details:
CVE-2025-5115 – HTTP/2 Denial of Service

- Severity: High
- CVSS Score: 7.5
- Description: Vulnerability in the bundled Jetty server ("MadeYouReset") allows unauthenticated attackers to cause denial-of-service if HTTP/2 is enabled (–http2Port). By default, HTTP/2 is disabled in official Jenkins installers and Docker images.

CVE-2025-59474 – Missing Permission Check (Sidepanel)

- Severity: Medium
- Description: Missing permission check in the sidepanel permits attackers lacking Overall/Read permission to list Jenkins agent names.

CVE-2025-59475 – Missing Permission Check (User Profile Dropdown)

- Severity: Medium
- Description: Missing permission check allows attackers without Overall/Read permission to access limited configuration data, such as available menu options and plugin presence.

CVE-2025-59476 – Log Message Injection

- Severity: Medium
- Description: Jenkins log formatter fails to restrict special characters in user-controlled log messages, enabling attackers to inject forged log lines and mislead administrators. While updates introduce indicators ([CR], [LF], [CRLF]) for injected line breaks, attackers may still use other characters (e.g., backspaces, Unicode Trojan Source).

Affected Versions

- Jenkins weekly up to and including 2.527
- Jenkins LTS up to and including 2.516.2

Fixed Versions

- Jenkins Weekly 2.528
- Jenkins LTS 2.516.3

RECOMMENDATIONS:

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

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://www.jenkins.io/security/advisory/2025-09-17/