



مجلس الأمن السيبراني
CYBER SECURITY COUNCIL



Multiple vulnerabilities in Jenkins

Tracking #:432318425

Date:20-02-2026



EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Jenkins core that could be exploited to execute unauthorized scripts within user sessions and potentially lead to the disclosure of sensitive project information.

TECHNICAL DETAILS:

Multiple vulnerabilities have been identified in Jenkins core that could allow authenticated users to perform stored cross-site scripting (XSS) attacks and access restricted build metadata. Exploitation may result in unauthorized script execution within user sessions and unintended disclosure of project information.

Vulnerability Details

Stored Cross-Site Scripting (XSS) in Node Offline Cause

- **CVE-2026-27099**
- **Severity:** High
- Improper input sanitization in the “Mark temporarily offline” node description allows user-supplied HTML to be rendered without escaping. An attacker with **Agent/Configure** or **Agent/Disconnect** permissions can inject malicious scripts that execute in other users’ browsers, potentially leading to session hijacking or unauthorized actions.

Build Information Disclosure via Run Parameter

- **CVE-2026-27100**
- **Severity:** Medium
- Insufficient permission validation in Run Parameter handling allows users to reference builds they are not authorized to access. This may enable attackers with **Item/Build** and **Item/Configure** permissions to determine the existence of jobs and builds and retrieve limited metadata.

Affected Products

- Jenkins weekly versions up to and including **2.550**
- Jenkins LTS versions up to and including **2.541.1**

Fixed Versions

- Jenkins weekly **2.551**
- Jenkins LTS **2.541.2**

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/2026-02-18/>