



مجلس الأمن السيبراني  
CYBER SECURITY COUNCIL



**Security Updates - Jenkins**

Tracking #:432316129

Date:09-08-2024

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 Jenkins released security updates to address multiple vulnerabilities in their products.

## TECHNICAL DETAILS:

### Vulnerability Details:

- **CVE-2024-43044** | Severity - **Critical** | Arbitrary file read vulnerability through agent connections can lead to RCE
  - Jenkins uses the Remoting library for the communication between controller and agents.
  - This library allows agents to load classes and classloader resources from the controller, so that Java objects sent from the controller (build steps, etc.) can be executed on agents.
  - This allows agent processes, code running on agents, and attackers with Agent/Connect permission to read arbitrary files from the Jenkins controller file system.
- **CVE-2024-43045** | Severity – Medium | Missing permission check allows accessing other users' "My Views"
  - Jenkins 2.470 and earlier, LTS 2.452.3 and earlier does not perform a permission check in an HTTP endpoint.
  - This allows attackers with Overall/Read permission to access other users' "My Views".
  - Attackers with global View/Configure and View/Delete permissions are also able to change other users' "My Views".

### Affected Versions:

- Jenkins weekly up to and including 2.470
- Jenkins LTS up to and including 2.452.3

### Fixed Versions:

- Jenkins weekly should be updated to version 2.471
- Jenkins LTS should be updated to version 2.452.4 or 2.462.1

## RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the security updates recently 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/2024-08-07/>