مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Vulnerabilities in Jenkins Docker Images

Tracking #:432317066

Date:11-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security vulnerabilities in Jenkins Docker images that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerabilities Details:

- **CVE-2025-32754 (jenkins/ssh-agent), CVE-2025-32755 (jenkins/ssh-slave)**
- Severity-Medium
- Critical vulnerabilities in the jenkins/ssh-agent and jenkins/ssh-slave Docker images related to SSH host key reuse. These vulnerabilities could allow attackers to impersonate build agents and potentially compromise the integrity of Jenkins pipelines.
- The affected Docker images automatically generate SSH host keys during image creation for Debian-based variants. This results in all containers derived from the same image version sharing identical SSH host keys. An attacker capable of intercepting network traffic between the Jenkins controller and build agents could impersonate a legitimate agent, enabling:
    - **Man-in-the-middle attacks**
    - **Credential theft**
    - **Injection of malicious code into pipelines**
    - **Unauthorized access to sensitive build data**

Affected Versions

- **jenkins/ssh-agent Docker images** up to and including 6.11.1
- **jenkins/ssh-slave Docker images** up to and including all versions

Fixed Versions:

- **jenkins/ssh-agent Docker images** version 6.11.2 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided 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/2025-04-10/