مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

United Arab Emirates

High-Severity Vulnerability in Kubernetes

Tracking #:432316542

Date:21-11-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability has been identified in Kubernetes that allows attackers to execute arbitrary commands beyond the container boundaries.

TECHNICAL DETAILS:

A high-severity vulnerability (CVE-2024-10220) has been identified in Kubernetes that allows attackers to execute arbitrary commands beyond the container boundaries

Vulnerability Details:

- CVE Identifier: CVE-2024-10220
- CVSS Score: 8.1 (High)
- Vulnerability Type: Arbitrary Command Execution
- Impact: The vulnerability allows a user with the ability to create a pod and associate a gitRepo volume to execute arbitrary commands beyond the container's boundary by manipulating the hooks folder within the target Git repository. This can lead to unauthorized access, privilege escalation, and potential compromise of the Kubernetes cluster.

Affected Versions: This issue affects Kubernetes clusters that use the gitRepo volume to clone Git repositories into pods. Specifically, the vulnerability impacts the following versions of kubelet:

- v1.30.0 to v1.30.2
- v1.29.0 to v1.29.6
- <= v1.28.11

Fixed Versions:

- master/v1.31.0 (fixes issue via restricting the gitRepo volume directory depth to a max of 1 level)
- v1.30.3 (fix applied via automated cherry-pick)
- v1.29.7 (fix applied via automated cherry-pick)
- v1.28.12(fix applied via automated cherry-pick)

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to Kubernetes cluster to one of the fixed versions listed above to prevent exploitation of this vulnerability.

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://github.com/kubernetes/kubernetes/issues/128885