مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Privilege Escalation Vulnerability in Kubernetes Armada

Tracking #:432316707

Date:07-01-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high severity vulnerability has been discovered in Karmada, a management platform designed for multi-cluster management across Kubernetes environments.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2024-56513**
- CVSS Base Score: 8.7 High
- Vulnerability Type: Incorrect Privilege Assignment (CWE-266)
- The vulnerability exists in the PULL mode cluster registration process of Karmada. When clusters are registered using the *karmadactl register* command, they are granted excessive privileges to access control plane resources.
- Exploiting this flaw allows an authenticated attacker to escalate privileges, potentially gaining administrative control over the entire federation system, which includes access to sensitive configuration data, disruption of application traffic scheduling, and lateral attacks across member clusters.

Affected Versions:

- Karmada versions prior to 1.12.0

Fixed Versions:

- Karmada version 1.12.0 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to update Karmada to the fixed version at the earliest.

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/karmada-io/karmada/security/advisories/GHSA-mg7w-c9x2-xh7r