مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Argo Events

Tracking #:432317086

Date:16-04-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Argo Events that could be exploited to escalate privileges and gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-32445
- CVSS Score 10.0 Critical
- A critical vulnerability exists in Argo Events, a popular event-driven workflow automation framework for Kubernetes. This vulnerability allows privilege escalation and potential host compromise through the manipulation of EventSource and Sensor custom resources (CRs).
- Users with permission to create or modify EventSource and Sensor CRs in Argo Events can exploit the spec.template and spec.template.container fields to specify arbitrary container properties. This includes enabling privileged mode, adding dangerous Linux capabilities, and mounting sensitive host filesystems.
- Successful exploitation can result in:
    - Privilege escalation to host and cluster level
    - Bypass of RBAC and Pod Security Policies
    - Breach of tenant isolation in multi-tenant clusters
    - Access to other tenants' data
    - Full host compromise

Affected Versions:

- Argo Events versions prior to **v1.9.6**

Fixed Version:

- Argo Events v1.9.6 and later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Argo Events.

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/argoproj/argo-events/security/advisories/GHSA-hmp7-x699-cvhq