مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in SUSE Rancher

Tracking #:432317150

Date:30-04-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in SUSE Rancher that could be exploited to gain unauthorized access to affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-22031**
- CVSS Score: 8.6 (High)
- A privilege escalation vulnerability exists in multiple versions of Rancher, an open-source container management platform. The flaw allows unauthorized privilege escalation across Kubernetes clusters due to namespace collisions caused by identical project names across clusters.
- This vulnerability arises from a namespace collision. When a user creates a project on one cluster with the same name as an existing project on another cluster, unauthorized access to resources in the other project becomes possible. This behavior is due to the use of project names as namespaces for storing resources.

Affected Versions:

- Rancher **prior to**:
  - v2.11.1
  - v2.10.5
  - v2.9.9

Fixed Versions:

- Rancher:
  - v2.11.1
  - v2.10.5
  - v2.9.9

RECOMMENDATIONS:

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

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/rancher/rancher/security/advisories/GHSA-8h6m-wv39-239m