مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Privilege Escalation Vulnerability in Rancher Fleet

Tracking #:432318919

Date:08-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical privilege escalation vulnerability, tracked as CVE-2026-41050, has been disclosed in Rancher Fleet, a GitOps platform widely used for managing Kubernetes clusters at scale.

TECHNICAL DETAILS:

A critical privilege escalation vulnerability, tracked as CVE-2026-41050, has been disclosed in Rancher Fleet, a GitOps platform widely used for managing Kubernetes clusters at scale.
The flaw allows attackers with limited repository access to bypass Fleet's multi-tenant isolation controls and gain effective cluster-admin privileges across downstream Kubernetes clusters. Exploitation enables unauthorized access to Kubernetes Secrets, credential theft, lateral movement, and full infrastructure compromise.

Vulnerability Details:

- CVE ID: CVE-2026-41050
- CVSS v3 Base Score: 9.9,Critical
- Affected Software: Rancher Fleet
- Issue Type: Privilege Escalation / Improper Impersonation Handling

Patched Versions:

- Rancher v2.14.1, v2.13.5, v2.12.9, and v2.11.13.
- For Rancher v2.10.11, users must manually update their Fleet deployment

RECOMMENDATIONS:

- Organizations operating shared Kubernetes or multi-tenant DevOps environments are at significant risk and should immediately patch affected versions, audit Git repositories, rotate exposed secrets, and enable enhanced Kubernetes audit logging.

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.tenable.com/cve/CVE-2026-41050