

مجلس الأمان السيبراني
CYBER SECURITY COUNCIL



United Arab Emirates

High-Severity Vulnerability in SUSE Rancher

Tracking #:432318349

Date:04-02-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLIGENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL



EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the SUSE Rancher that could allow TLS protections to be bypassed during login, potentially exposing sensitive authentication data.

TECHNICAL DETAILS:

A high-severity vulnerability exists in Rancher Manager where the Rancher CLI login command may bypass TLS verification when using self-signed certificates with the --skip-verify flag. Attackers with network access could exploit this to intercept authentication credentials and bypass TLS security controls.

Vulnerability Details

- **CVE-2025-67601**
- **CVSS Score 8.4** High
- A vulnerability exists in the Rancher CLI login command when the --skip-verify flag is used without specifying the --cacert option while connecting to Rancher Manager with self-signed certificates. In this scenario, the CLI attempts to retrieve CA certificates from Rancher's internal cacerts setting.
- An attacker with network-level access between the Rancher CLI and Rancher Manager could exploit this behavior to interfere with the TLS handshake and supply a malicious CA certificate. Successful exploitation may enable Man-in-the-Middle (MITM) attacks, resulting in TLS bypass and potential exposure of authentication credentials.

Affected Versions

- 2.13.0 to prior to 2.13.2
- 2.12.0 to prior to 2.12.6
- 2.11.0 to prior to 2.11.10
- 2.10.0 to prior to 2.10.11

Fixed Versions

- v2.13.2, v2.12.6, v2.11.10, and v2.10.11

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by SUSE 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-mc24-7m59-4q5p>