مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerabilities in SUSE Rancher

Tracking #:432316929
Date:04-03-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that SUSE has released security advisories addressing two high-severity vulnerabilities in Rancher, an open-source container management platform. These vulnerabilities could allow attackers to launch denial-of-service (DoS) attacks and impersonate users.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-23388 (CVSS 8.2): Unauthenticated Stack Overflow in /v3-public/authproviders API**
  - This vulnerability allows an unauthenticated attacker to crash the Rancher server by submitting malicious data to the /v3-public/authproviders API endpoint. While the attacker cannot write incorrect data to the API, the DoS attack can disrupt services and prevent legitimate users from accessing the platform.
- **CVE-2025-23389 (CVSS 8.4): Improper Account Binding Validation in SAML Authentication**
  - This vulnerability enables a local user to impersonate any other user on Rancher by manipulating cookie values during their initial login through a SAML authentication provider. An attacker could exploit this flaw to gain unauthorized access to sensitive data and perform administrative actions.

Affected Versions:

- Rancher versions v2.8.12 and earlier
- Rancher versions v2.9.6 and earlier
- Rancher versions v2.10.2 and earlier

Fixed Versions:

- Rancher v2.8.13
- Rancher v2.9.7
- Rancher v2.10.3

RECOMMENDATIONS:

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

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-xr9q-h9c7-xw8q
- https://github.com/rancher/rancher/security/advisories/GHSA-mq23-vvg7-xfm4