مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Rancher

Tracking #:432316444

Date:28-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability affecting Rancher's handling of vSphere credentials. This vulnerability exposes sensitive vSphere Cloud Provider Interface (CPI) and Container Storage Interface (CSI) credentials in plaintext within Rancher configuration objects.

TECHNICAL DETAILS:

A vulnerability has been identified in the way that Rancher stores vSphere's CPI (Cloud Provider Interface) and CSI (Container Storage Interface) credentials used to deploy clusters through the vSphere cloud provider. This issue leads to the vSphere CPI and CSI passwords being stored in a plaintext object inside Rancher. This vulnerability is only applicable to users that deploy clusters in vSphere environments.

- **CVE ID: CVE-2022-45157**
- **CVSS Score**: 9.1,Critical
- Unauthorized access to sensitive vSphere credentials.
- Potential exposure of credentials in downstream cluster filesystems to privileged users.

Affected Versions:

- Rancher 2.7.0-2.9.2

Fixed Versions:

- Rancher 2.8.9 and 2.9.3

RECOMMENDATIONS:

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

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-xj7w-r753-vj8v