مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in SUSE Rancher

Tracking #:432316450

Date:29-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in SUSE Rancher that could potentially be exploited to execute malicious code on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-22036**
- CVSS score of 9.1 Critical
- A remote code execution (RCE) vulnerability exists in SUSE Rancher, which allows attackers to exploit cluster and node drivers to escape the chroot jail and gain root access within the Rancher container.
- The vulnerability stems from several issues in Rancher's handling of drivers:
  - **Path Manipulation**: Rancher adds /opt/drivers/management-state/bin to the PATH environment variable during startup, expanding the attack surface for malicious drivers.
  - **Improper File Ownership**: Critical binaries like /usr/bin/rancher-machine, /usr/bin/helm_v3, and /usr/bin/kustomize are assigned to UID 1001 and GID 127 instead of root.
  - **Symbolic Link Exploitation**: Lack of file type validation allows attackers to register malicious drivers using symbolic links.
- Successful exploitation of this vulnerability could lead to: gaining root access to the Rancher container, escalating privileges within the container, and potentially escaping the container and accessing the host system in development/test environments with privileged Docker setups.

Affected Versions:

- Rancher versions prior to 2.7.16
- Rancher versions prior to 2.8.9
- Rancher versions prior to 2.9.3

Fixed Versions:

- Rancher version 2.7.16
- Rancher version 2.8.9
- Rancher version 2.9.3

RECOMMENDATIONS:

- **Upgrade Immediately:** Update to fixed versions as soon as possible
- **Use Trusted Drivers Only**: Limit driver execution to vetted, trusted sources
- **Restrict Admin Privileges**: Limit access to trusted users for both Admins and Restricted Admins
- **Monitor for Suspicious Activity:** Implement robust logging and monitoring to detect potential exploitation attempts.
- **Review Security Configurations:** Assess and tighten security settings, especially in development and test environments.

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-h99m-6755-rgwc