مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in SUSE Manager

Tracking #:432317560

Date:01-08-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in SUSE Manager that could be exploited to execute malicious code on affected systems, potentially leading to full system compromise.

TECHNICAL DETAILS:

A critical vulnerability has been identified in SUSE Manager that allows unauthenticated remote attackers to execute arbitrary commands as root. The flaw arises from a missing authentication mechanism on the websocket endpoint /rhn/websocket/minion/remote-commands, permitting full system compromise without the need for credentials or user interaction.

This vulnerability affects multiple deployment types, including containerized and cloud-based instances, and poses a severe risk to enterprise environments relying on SUSE Manager for infrastructure and configuration management.

Vulnerability Details:

- **CVE ID**: CVE-2025-46811
- **CVSS 4.0 Score**: 9.3 (Critical)
- The vulnerability stems from an authentication bypass in SUSE Manager's websocket interface. Specifically, the endpoint /rhn/websocket/minion/remote-commands fails to enforce proper authentication, allowing any actor with network access to this route to issue arbitrary commands as the root user. Exploitation requires no prior access and offers unrestricted control over the system.
- Exploitation of CVE-2025-46811 could allow attackers to:
  - Install persistent backdoors or malware
  - Exfiltrate sensitive data or credentials
  - Modify or destroy critical system configurations
  - Use compromised hosts as pivot points for lateral movement

Affected Versions:

- Multiple versions of SUSE Manager, including Container versions 5.0.5.7.30.1, various SLES15-SP4-Manager-Server images, and SUSE Manager Server Module 4.3.
- Multiple SUSE Manager configurations, including containerized deployments and various cloud platform images for Azure, EC2, and Google Cloud Engine

RECOMMENDATIONS:

- Patch Immediately: Apply the latest security updates to all affected systems.
- Restrict Network Access: Use firewall rules or access controls to block external access to the /rhn/websocket/minion/remote-commands endpoint.
- Audit Systems: Review logs and activity for signs of compromise, particularly on exposed or internet-accessible instances.
- Isolate Unpatched Systems: Temporarily remove vulnerable instances from production networks if patches cannot be immediately applied.
- Monitor for unexpected root-level activity
- Conduct internal vulnerability scans to locate all affected SUSE Manager deployments

- Implement segmentation between administrative interfaces and general network zones

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://nvd.nist.gov/vuln/detail/CVE-2025-46811
- https://www.suse.com/security/cve/CVE-2025-46811.html