Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Critical SUSE Manager Vulnerability Allows Remote Command Execution as Root

Vulnerability Note: VN-2025-14

Date of Issue: 01 August 2025

Severity Rating: High

Systems Affected:

The vulnerability affects 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.

Description

A critical security vulnerability has been discovered in SUSE Manager that enables attackers to execute arbitrary commands with root privileges without any authentication. The vulnerability is caused due to a missing authentication mechanism for a critical function within SUSE Manager's websocket interface. This vulnerability can allow anyone with network access to the /rhn/websocket/minion/remote-commands endpoint and execute arbitrary commands as the root user. Attackers require no special privileges or user interaction to exploit this vulnerability, making it particularly dangerous.

The vulnerability also impacts multiple SUSE Manager configurations, including containerized deployments and various cloud platform images for Azure, EC2, and Google Cloud Engine.

CVE Information
CVE-2025-46811

Workaround

Organisations should immediately identify all SUSE Manager instances in their environments and prioritize patching efforts. SUSE has released security updates addressing this vulnerability. More information is available on:
https://bugzilla.suse.com/show_bug.cgi?id=CVE-2025-46811

Organizations must upgrade to the latest patched versions immediately and implement network-level controls to restrict access to the websocket endpoint until patches can be applied.

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,