July 17, 2024

Overall Rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of Cisco publishing a security advisory to address a vulnerability in OpenSSH Server which is used in multiple products and in the RADIUS protocol which is used in multiple products.

Technical Details

A vulnerability in the authentication system of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an unauthenticated, remote attacker to change the password of any user, including administrative users.

This vulnerability is due to improper implementation of the password-change process. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow an attacker to access the web UI or API with the privileges of the compromised user.

Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.

This vulnerability is rated as a **CRITICAL** risk. Software updates exist to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have at vulnerabilityandriskmanagement@gov.bc.ca

References

- **CVE-2024-6387 CVE-2024-20401 CVE-2024-20419 CVE-2024-20435 CVE-2024-20296 CVE-2024-20323 CVE-2024-20395 CVE-2024-20396 CVE-2024-20416 CVE-2024-20400 CVE-2024-20429 CVE-2024-3596 CVE-2024-6387 CVE-2024-20456 CVE-2024-20399**
- OpenSSH security advisory (AV24-366)
- Cisco Security Advisory – cisco-sa-openssh-rce-2024
- Cisco Security Advisories
- Alert - RADIUS Protocol Susceptible to Forgery Attacks