July 12, 2024

Overall Rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware Qualys Threat Research Unit (TRU) disclosed an unauthenticated, remote code execution vulnerability that affects the OpenSSH server (sshd) in glibc-based Linux systems. Cisco is investigating its product line to determine which products and cloud services may be affected by this vulnerability.

Technical Details

The impact of this vulnerability may allow <details, hyperlink>.

Exploitability Metrics
Attack Vector: Network
Attack Complexity: High
Privileges Required: None
User Interaction: None

Cisco products that are affected are available in a table under Vulnerable Products - and are available in a table format Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion): July 2024.

If a future release date is indicated for software, the date provided represents an estimate based on all information known to Cisco as of the Last Updated date at the top of the advisory. Availability dates are subject to change based on several factors, including satisfactory testing results and delivery of other priority features and fixes. If no version or date is listed for an affected component (indicated by a blank field and/or an advisory designation of Interim), Cisco is continuing to evaluate the fix and will update the advisory as additional information becomes available.

This vulnerability is rated as a **HIGH** risk. A software update exists to address this risk.

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 atVulnerabilityandRiskManagement@gov.bc.ca.

References

- CVE-2024-6387
- Remote Unauthenticated Code Execution Vulnerability in OpenSSH Server (regreSSHion): July 2024
- VRM Vulnerability Reports