July 4, 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 of a Citrix Cloud Software Group OpenSSH vulnerability. The vulnerability affects NetScaler Console (formerly Citrix ADM). Citrix is currently investigating other products for this vulnerability including NetScaler (formerly Citrix ADC), NetScaler Gateway (formerly Citrix Gateway), Citrix Endpoint Management, Citrix Hypervisor, Citrix Secure Private Access.

Technical Details

Cloud Software Group is aware of the vulnerability CVE-2024-6387 impacting OpenSSH. Qualys has discovered a remote unauthenticated code execution vulnerability in OpenSSH's server (sshd) in glibc-based Linux systems. Because this vulnerability is a regression of the previously patched vulnerability CVE-2006-5051, which was reported in 2006, it is being referred to as regreSSHion. The vulnerability has been assigned the CVE identifier CVE-2024-6387.

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

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, CVE-2006-5051
- N24 -275 OpenSSH Security Advisory
- Cloud Software Group Security Advisory for CVE-2024-6387
- VRM Vulnerability Reports