July 3, 2024

Overall Rating: HIGH

This is a technical bulletin intended for technical audiences.

Summary

An OpenSSH unauthenticated remote code execution (RCE) vulnerability aka "regreSSHion" may allow root privileges on glibc-based Linux systems. This is assessed as a critical vulnerability and impacts OpenSSH versions between 8.5p1 and 9.

Technical Details

The vulnerability is being tracked as CVE-2024-6387, is due to a signal handler race condition in sshd that may allow an unauthenticated remote attacker to execute arbitrary code as root. Reports are this vulnerability is possibly a regression of the previously patched OpenSSH vulnerability (CVE-2006-5051).

Successful exploitation has been demonstrated on 32-bit Linux/glibc systems with ASLR. Under lab conditions, the attack requires on average 6-8 hours of continuous connections up to the maximum the server will accept. Exploitation on 64-bit systems is believed to be possible but has not been demonstrated at this time.

OpenBSD is not vulnerable.

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
- OpenSSH 9.8 was released on 2024-07-01
- OpenSSH
- An Unauthenticated Remote Code Execution (RCE) vulnerability in OpenSSH's server (sshd) on glibc-based Linux systems
- VRM Vulnerability Reports