ORNA™

Cybersecurity Advisory

Dear ORNA Customer,

We are sending you this advisory to provide situational awareness about the critical unauthenticated remote code execution vulnerability in OpenSSH: CVE-2024-6387.

Summary

A critical unauthenticated remote code execution vulnerability has been identified in OpenSSH's server component on glibc-based Linux systems. Assigned CVE-2024-6387 and codenamed *regreSSHion*, this vulnerability enables attackers to gain full root access without user interaction. It impacts OpenSSH versions 8.5p1 through 9.7p1, as well as versions earlier than 4.4p1 unless patched for CVE-2006-5051 and CVE-2008-4109.

Overview

Discovered by the Qualys Threat Research Unit, *regreSSHion* stems from a signal handler race condition in the OpenSSH server. This flaw allows an attacker to execute arbitrary code with root privileges on affected systems. It reintroduces a previously patched vulnerability (CVE-2006-5051) in October 2020 as part of OpenSSH version 8.5p1.

regreSSHion is exploitable under certain conditions, where the vulnerability manifests when sshd's *SIGALRM* handler is called asynchronously if a client does not authenticate within the time specified by the LoginGraceTime setting. Exploitation requires sustained connections, typically 6-8 hours of continuous attempts.

The exploit does not require authentication or user interaction and impacts the default configuration of sshd, making it a significant security risk. Successful exploitation requires prolonged connections and affects systems with address space layout randomization enabled.

The risk impact includes unauthenticated remote code execution leading to full root access, potential for sensitive data exfiltration, ability to establish backdoors and maintain unauthorized access and execution of malicious code and installation of malware.

Affected Versions

- OpenSSH versions 8.5p1 to 9.7p1.
- Versions earlier than 4.4p1, if not patched for CVE-2006-5051 and CVE-2008-4109.
- OpenBSD systems are unaffected due to a built-in security mechanism. The impact on macOS and Windows systems is currently unconfirmed and under analysis.

Recommendations

Recommendation #1: Update OpenSSH

Upgrade to OpenSSH version 9.8p1 or later, where the vulnerability has been addressed.

Recommendation #2: Restrict SSH Access

Implement network-based controls to limit SSH access and enforce network segmentation.

Recommendation #3: Monitor and Detect
Utilize IoCs provided by Qualys to detect potential exploitation attempts.

Recommendation #4: Prepare for the Worst
ORNA **strongly recommends** that organizations ensure that all critical systems are backed up appropriately and that incident response plans are rehearsed regularly so that all participants understand their role.

References

1. Security Tracker: https://security-tracker.debian.org/tracker/CVE-2024-6387
2. Qualys: https://www.qualys.com/regresshion-cve-2024-6387/
3. The Hacker News: https://thehackernews.com/2024/07/new-openssh-vulnerability-could-lead-to.html
4. Security Week: https://www.securityweek.com/millions-of-openssh-servers-potentially-vulnerable-to-remote-regresshion-attack/

If you have any additional questions, please reach out to your ORNA representative at sme@orna.app.

Sincerely,
ORNA Team