

Security Advisory 2024-066

Critical Vulnerability in OpenSSH

July 1, 2024 — v1.0

TLP:CLEAR

History:

- 01/07/2024 — v1.0 – Initial publication

Summary

On July 1, 2024, a new OpenSSH unauthenticated remote code execution (RCE) vulnerability dubbed *regreSSHion* was reported, affecting glibc-based Linux systems. This vulnerability, identified as **CVE-2024-6387**, allows remote attackers to execute arbitrary code as root due to a signal handler race condition in `sshd` [1].

Technical Details

This vulnerability, if exploited, could lead to full system compromise, where an attacker can execute arbitrary code with the highest privileges, resulting in a complete system takeover, installation of malware, data manipulation, and the creation of backdoors for persistent access. It could facilitate network propagation, allowing attackers to use a compromised system as a foothold to traverse and exploit other vulnerable systems within the organization [2].

Affected Products

The *regreSSHion* flaw impacts OpenSSH servers on Linux from version 8.5p1 up to, but not including 9.8p1 [1].

Versions 4.4p1 up to, but not including 8.5p1 are not vulnerable to **CVE-2024-6387** thanks to a patch for CVE-2006-5051, which secured a previously unsafe function [1].

Versions older than 4.4p1 are vulnerable to *regreSSHion* unless they are patched for CVE-2006-5051 and CVE-2008-4109. OpenBSD systems are not impacted by this flaw thanks to a secure mechanism introduced back in 2001 [1].

Recommendations

CERT-EU recommends to review and apply the patches from Linux distribution security bulletins, including but not limited to:

- Ubuntu [3]
- Debian [4]
- RedHat [5]

However, if it cannot be updated immediately, set the `LoginGraceTime` to 0 in the `sshd` configuration file, but note that this can expose the server to denial-of-service attacks [1].

References

[1] <https://www.bleepingcomputer.com/news/security/new-regresshion-openssh-rce-bug-gives-root-on-linux-servers/>

[2] <https://blog.qualys.com/vulnerabilities-threat-research/2024/07/01/regresshion-remote-unauthenticated-code-execution-vulnerability-in-openssh-server>

[3] <https://ubuntu.com/security/CVE-2024-6387>

[4] <https://security-tracker.debian.org/tracker/CVE-2024-6387>

[5] <https://access.redhat.com/security/cve/cve-2024-6387>