OpenSSH vulnerability CVE-2024-6387

724 Nesvin KN July 17, 2024 Common Errors & Troubleshooting 1638

How to fix the OpenSSH vulnerability CVE-2024-6387?

Synopsis: CVE-2024-6387, known as **regreSSHion**, has been discovered in the OpenSSH server. This vulnerability allows remote unauthenticated attackers to execute arbitrary code on the target server, posing a significant threat to systems that use OpenSSH for secure communications.

NOTE:

This is a vulnerability in the OpenSSH software package that ships with the OS (Ubuntu, CentOS, RockyLinux, Debian, etc) and NOT in the Ezeelogin software. We would however recommend you to apply the fix on the server if your OpenSSH version falls in the vulnerable versions .

RegreSSHion vulnerability affected OpenSSH versions:

- Versions before 4.4p1
- Versions 8.5p1 to 9.7p1(inclusive)

How to fix regreSSHion vulnerability?

Method 1: Upgrade OpenSSH version to 9.8.

Check the current running openssh version:

Method 2: The issue can be resolved by setting the **LoginGraceTime parameter to 0** in the sshd configuration file.

2.a: Login to the server as root user and edit the sshd configuration file.

2.b: Syntax check the sshd configuration file before restarting the service.

2.c: Restart sshd service to set the changes.

Default OpenSSH version in different OS's:

Find the OpenSSH version by running the command (sshd -V).

Ubuntu 24	OpenSSH_9.6p1 Ubuntu-3ubuntu13, OpenSSL 3.0.13 30 Jan 2024
Ubuntu 22	OpenSSH_8.9p1 Ubuntu-3ubuntu0.6, OpenSSL 3.0.2 15 Mar 2022
Ubuntu 20	OpenSSH 8.2p1
Ubuntu 18	OpenSSH 7.6p1
RockyLinux 9 / RHEL 9 / AlmaLinux 9	OpenSSH_8.7p1, OpenSSL 3.0.7 1 Nov 2022
RockyLinux 8 / RHEL 8 / AlmaLinux 8 / CentOS 8	OpenSSH_7.8p1, OpenSSL 1.1.1k FIPS 25 Mar 2021
Debian 11	OpenSSH 8.4
Debian 10	OpenSSH 7.9p1
CentOS 7	OpenSSH_7.4p1, OpenSSL 1.0.2k-fips 26 Jan 2017

Note :-

The sshd server will still be vulnerable to Denial-of-Service attacks due to the possibility of MaxStartups connection exhaustion, however it'll be safe against possible remote code execution attacks. Therefore, It is recommended to put the Ezeelogin gateway server behind a VPN or firewall to mitigate this.

References :

1. https://www.cve.org/CVERecord?id=CVE-2024-6387
2. https://access.redhat.com/security/cve/CVE-2024-6387
3. https://nvd.nist.gov/vuln/detail/CVE-2024-6387
4. https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt

Related Article

1. How to Upgrade OpenSSH in CentOS