

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

regreSSHion: Exploiting Signal Handler Race Condition in OpenSSH

Date of Publication

July 2, 2024

Admiralty Code

A1

TA Number

TA2024251




Summary

First Seen: July 1, 2024

Affected Product: OpenSSH server

Impact: The "regreSSHion" vulnerability (CVE-2024-6387) in OpenSSH allows unauthenticated remote code execution with root privileges on glibc-based Linux systems, affecting versions 8.5p1 to 9.7p1. Despite being hard to exploit, it poses severe risks including full system compromise. Mitigation includes updating to version 9.8p1 or adjusting 'LoginGraceTime' settings, though this may expose systems to denial-of-service attacks.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-6387	regreSSHion (OpenSSH Unauthenticated Remote Code Execution Vulnerability)	OpenSSH server			

Vulnerability Details

#1

A critical vulnerability, dubbed "regreSSHion" (CVE-2024-6387), has been identified in OpenSSH, impacting glibc-based Linux systems. This flaw, allows unauthenticated remote attackers to execute arbitrary code with root privileges due to a signal handler race condition in sshd. Despite its severity, exploiting regreSSHion is challenging, though AI tools could increase the success rate.

#2

OpenSSH is widely used for secure remote login, server management, and file transfers. The vulnerability affects OpenSSH versions from 8.5p1 up to 9.8p1, while versions 4.4p1 to 8.5p1 are protected by a previous patch. Older versions are vulnerable unless similarly patched for CVE-2006-5051 and CVE-2008-4109. OpenBSD systems are secure against this flaw, and its impact on macOS and Windows remains uncertain.

#3

With the recent availability of a Proof of Concept (PoC) exploit, potential threat actors may attempt to weaponize it in real-world attacks. To mitigate this risk, users should promptly update to OpenSSH 9.8p1, which addresses the vulnerability. Additional mitigation strategies include restricting SSH access via network controls and setting 'LoginGraceTime' to 0 if immediate updates are not feasible, though this can expose the server to denial-of-service attacks.

#4

Over 14 million internet-exposed OpenSSH servers have been detected, with 700,000 confirmed vulnerable. Updating to the latest patched version of OpenSSH is crucial to protect your infrastructure from potential exploitation and ensure the security of your systems.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-6387	OpenSSH versions earlier than 4.4p1 OpenSSH versions from 8.5p1 to before 9.8p1	cpe:2.3:a:openssh:openssh:*:*:*:*:*	CWE-364

Recommendations



Update OpenSSH: Upgrade your OpenSSH server to version 9.8p1 or later, which includes a fix for the vulnerability. If immediate updating is not possible, set the 'LoginGraceTime' parameter to 0 in the sshd configuration file. Be aware that this could expose your server to denial-of-service (DoS) attacks.



Restrict SSH Access: Implement network-based controls such as firewalls to restrict SSH access. Use network segmentation to limit the spread of any potential compromise.



Monitor and Audit: Regularly scan your systems for vulnerable OpenSSH versions using tools like Shodan and Censys. Conduct frequent security audits and monitor logs for unusual SSH activity.



Best Practices: Follow general security best practices, such as keeping software and firmware up to date, using strong authentication mechanisms, and employing endpoint protection solutions.

Potential MITRE ATT&CK TTPs

<u>TA0001</u> Initial Access	<u>TA0002</u> Execution	<u>TA0004</u> Privilege Escalation	<u>TA0042</u> Resource Development
<u>T1059</u> Command and Scripting Interpreter	<u>T1190</u> Exploit Public-Facing Application	<u>T1203</u> Exploitation for Client Execution	<u>T1068</u> Exploitation for Privilege Escalation
<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits	

Patch Details

Upgrade OpenSSH to the latest version 9.8p1 or later

<https://www.openssh.com/ftp.html>

<https://www.openssh.com/releasesnotes.html>

References

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

<https://www.qualys.com/2024/07/01/cve-2024-6387/regresshion.txt>

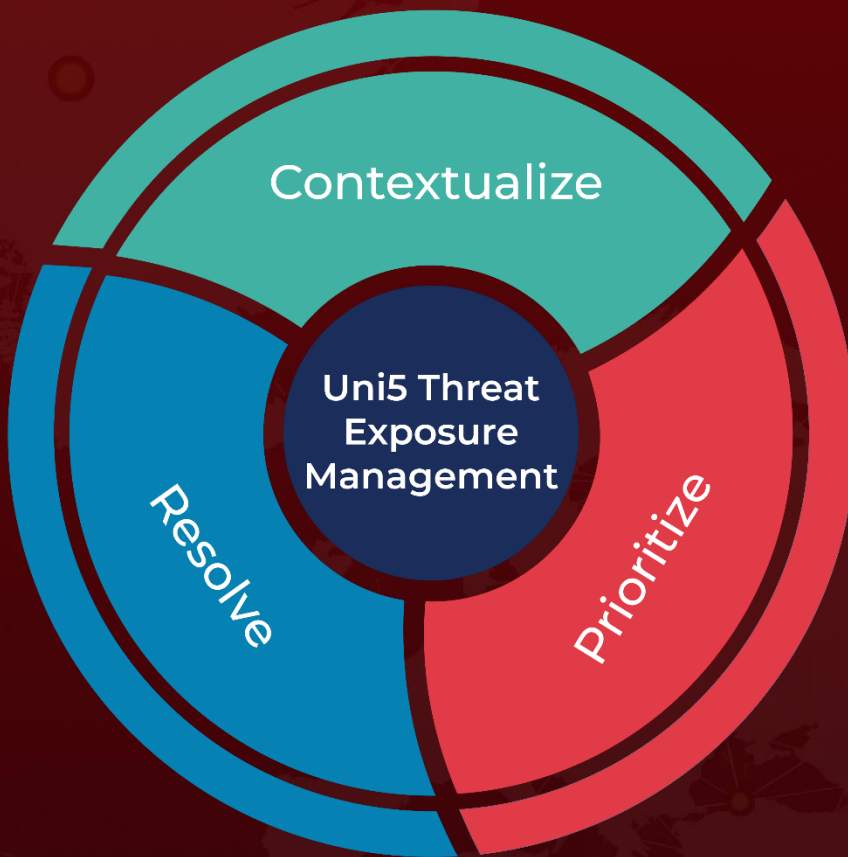
<https://github.com/zgzhang/cve-2024-6387-poc>

<https://github.com/acrono/cve-2024-6387-poc>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

July 2, 2024 • 7:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com