GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

14 September 2026

Advisory 311: OpenSSH "regreSSHion" Signal Handler Race Condition Remote Code Execution - Still Being Detected on Internet-Exposed Servers (CVE-2024-6387).

Release Date: 1st July 2024
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate an OpenSSH server on a glibc-based Linux system. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2024-6387, known as "regreSSHion," is a critical remote code execution vulnerability in OpenSSH's server daemon (sshd), publicly disclosed on 1 July 2024. It is a regression of a 2006 vulnerability (CVE-2006-5051): a protective code path was accidentally removed in OpenSSH 8.5p1 (released March 2021), reintroducing a signal handler race condition present between OpenSSH 8.5p1 and 9.7p1. CERTVU is issuing this advisory now, more than two years after original disclosure, because CVE-2024-6387 continues to appear in the Shadowserver Foundation's "Accessible SSH" internet-scanning report, which CERTVU monitors on a recurring basis, a clear trend of internet-facing Linux servers still running an unpatched, vulnerable OpenSSH version well after a fix has been available, consistent with the same "vulnerable configuration or software version persists long after a patch exists" pattern seen in this session's Terrapin advisory (Advisory 310).

What are the systems affected?

The following version(s) are affected:

- OpenSSH 8.5p1 through 9.7p1, on glibc-based Linux systems – (Affected)

OpenSSH 9.8p1 and later – (Not affected, patched); OpenSSH on OpenBSD, and OpenSSH for Windows – (Not affected)

Upgrade OpenSSH to version 9.8p1 or later on every glibc-based Linux server. Where an immediate upgrade is not possible, setting "LoginGraceTime 0" in sshd_config is a documented interim mitigation (note this can expose the server to a denial-of-service risk from held-open connections, so treat it as temporary only), or apply your Linux distribution's own backported patch if one has been issued.

What does this mean?

Typical attack flow:

1. **Repeatedly open connections that fail to authenticate within the grace period**
    - A remote, unauthenticated attacker repeatedly opens SSH connections to a vulnerable server and lets each one fail to authenticate within the default 120-second LoginGraceTime window, triggering sshd's SIGALRM handler under race-condition-favorable timing.
2. **Win the race condition and execute arbitrary code**
    - When the signal handler's unsafe function calls execute at just the right moment relative to the main process's memory state, the attacker can achieve memory corruption and ultimately execute arbitrary code, typically with root privileges, since sshd runs as root before privilege separation completes.

Attack vectors:

- A network-based, unauthenticated attack against any glibc-based Linux system running a vulnerable OpenSSH version with its SSH port reachable from an untrusted network.
- No user interaction or privileges are required, though attack complexity is high (CVSS AC:H) given the race condition typically requires several hours of sustained connection attempts. CERTVU is not aware of confirmed, widespread active exploitation of this specific CVE at the time of writing, but its continued detection in Shadowserver's Accessible SSH internet-scanning report.

Successful exploitation may allow attackers to:

- Execute arbitrary code on a vulnerable Linux server, typically with root privileges, without any authentication.
- Fully compromise the affected server and use it as a foothold to pivot into the wider network it is connected to.

Mitigation process

CERTVU recommends the following:

1. Upgrade OpenSSH immediately

- Upgrade OpenSSH to version 9.8p1 or later, or apply your Linux distribution's own backported fix, on every glibc-based Linux server.

2. Apply the interim LoginGraceTime workaround only where an immediate upgrade is not possible
3. Restrict SSH exposure where a full upgrade must be scheduled

Report any suspected compromise involving SSH access to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2024-6387
2. https://github.com/advisories/GHSA-2x8c-95vh-gfv4