CVE-2025-26465 AND CVE-2025-26466: OPENSSH VULNERABILITIES LEADING TO MITM AND DDOS ATTACKS

Vairav Advisory Report

Date: 02-19-2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

Thirbam Sadak 148
Baluwatar, Kathmandu

EXECUTIVE SUMMARY

Two vulnerabilities, CVE-2025-26465 and CVE-2025-26466, have been identified in OpenSSH, a widely used suite for secure network communications. CVE-2025-26465 allows for machine-in-the-middle (MitM) attacks, while CVE-2025-26466 enables pre-authentication denial-of-service (DoS) attacks. Exploitation of these vulnerabilities could result in system compromise, data exposure, and service disruption.

VULNERABILITY DETAILS

CVE-2025-26465:

- **Description:** This vulnerability arises when the VerifyHostKeyDNS option is enabled in the OpenSSH client. An attacker capable of performing a MitM attack can impersonate a legitimate server by bypassing the client's host key verification, leading to unauthorized access.
- **Impact:** Successful exploitation allows attackers to intercept or modify data transmitted over SSH, potentially leading to credential theft, unauthorized data access, and further network compromise.
- **CVSS Score:** 6.8 (Medium)

CVE-2025-26466:

- **Description:** This flaw affects both OpenSSH clients and servers, enabling attackers to cause excessive memory and CPU consumption through pre-authentication processes. By sending specially crafted SSH handshake messages, an attacker can exhaust system resources, leading to service unavailability.
- **Impact:** Exploitation can result in prolonged service outages, preventing legitimate users from accessing SSH services and hindering administrative operations.
- **CVSS Score:** 9.8 (Critical)

AFFECTED VERSIONS

OpenSSH versions affected by these vulnerabilities include:

- **CVE-2025-26465:** Versions 6.8p1 through 9.9p1
- **CVE-2025-26466:** Versions 9.5p1 through 9.9p1

EXPLOIT DETAILS

These vulnerabilities are particularly concerning in environments where OpenSSH is utilized for secure remote administration and file transfers.

- **CVE-2025-26465:** An attacker positioned between the client and server can exploit the VerifyHostKeyDNS option to impersonate the server, leading to potential data breaches and unauthorized system access.
- **CVE-2025-26466:** By initiating multiple malicious SSH handshake requests, an attacker can deplete server resources, causing denial-of-service conditions that disrupt critical operations.

RECOMMENDED ACTIONS

- Upgrade to OpenSSH version 9.9p2 or later to address these vulnerabilities.
- Ensure the VerifyHostKeyDNS option is disabled unless explicitly required.
- Implement server-side configurations such as LoginGraceTime, MaxStartups, and PerSourcePenalties to mitigate potential DoS attacks.

ADDITIONAL SECURITY MEASURES

- **Network Monitoring**: Continuously monitor network traffic for unusual activities indicative of MitM or DoS attacks.
- **Access Controls**: Restrict SSH access to trusted networks and employ multi-factor authentication to enhance security.
- **Regular Audits**: Conduct periodic security assessments to identify and remediate potential vulnerabilities in SSH configurations.

REFERENCES

- https://thehackernews.com/2025/02/new-openssh-flaws-enable-man-in-middle.html
- https://blog.qualys.com/vulnerabilities-threat-research/2025/02/18/qualys-tru-discovers-two-vulnerabilities-in-openssh-cve-2025-26465-cve-2025-26466
- https://www.upwind.io/feed/openssh-vulnerabilities-cve-2025-26465-and-cve-2025-26466-enable-man-in-the-middle-and-dos-attacks

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com