مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Vulnerabilities in OpenSSH

Tracking #:432316882

Date:19-02-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers reported two critical vulnerabilities in OpenSSH, which affect both the OpenSSH client and server.

TECHNICAL DETAILS:

Two critical vulnerabilities identified in OpenSSH, which affect both the OpenSSH client and server, tracked as CVE-2025-26465 and CVE-2025-26466. These flaws expose OpenSSH clients and servers to machine-in-the-middle (MITM) attacks and pre-authentication denial-of-service (DoS) attacks, respectively.

Details:

1. **CVE-2025-26465 - Active Machine-in-the-Middle Attack on OpenSSH Client:**
   - **Vulnerability Description:** This vulnerability affects the OpenSSH client when the VerifyHostKeyDNS option is enabled. The option allows the SSH client to look up and verify a server's host key using DNS records (specifically SSHFP records). The vulnerability enables a machine-in-the-middle attack, where attackers can intercept and manipulate SSH connections.
   - **Attack Details:** The attack succeeds regardless of whether the VerifyHostKeyDNS option is set to "yes" or "ask" (its default value is "no"). It does not require user interaction and does not rely on the existence of an SSHFP resource record in DNS. Although the VerifyHostKeyDNS option is disabled by default, it was enabled by default on FreeBSD systems from September 2013 until March 2023.
   - **Impact:** Successful exploitation of this vulnerability allows attackers to perform man-in-the-middle attacks on OpenSSH clients, potentially leading to unauthorized access, data theft, or further exploitation of vulnerable systems.

2. **CVE-2025-26466 - Pre-authentication Denial-of-Service Attack:**
   - **Vulnerability Description:** This vulnerability affects both the OpenSSH client and server, enabling attackers to initiate a pre-authentication denial-of-service attack that results in asymmetric consumption of memory and CPU resources. The vulnerability was introduced in August 2023, shortly before the release of OpenSSH 9.5p1.
   - **Attack Details:** The pre-authentication DoS attack consumes resources disproportionately, leading to a potential service outage or degraded system performance. Attackers can trigger this vulnerability without authentication, making it easier to launch attacks against OpenSSH servers.
   - **Impact:** Successful exploitation of this vulnerability can result in severe performance degradation, service outages, or even crashes of vulnerable OpenSSH servers.

- **Affected versions:**
  - OpenSSH versions from 6.8p1 through 9.9p1 are vulnerable to CVE-2025-26465, the flaw introduced in December 2014.
  - OpenSSH versions 9.5p1 through 9.9p1 are vulnerable to CVE-2025-26466, the flaw introduced in August 2023.

- **Fixed Versions:**
  - OpenSSH 9.9p2

RECOMMENDATIONS:

- Upgrade OpenSSH immediately to fixed version to mitigate these threats.
- Review SSH configurations to ensure security settings are properly enforced.
- Deploy intrusion detection systems (IDS) to detect and block suspicious SSH traffic and use firewalls to restrict SSH access to trusted IP addresses.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.openssh.com/releasenotes.html