

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Is Your Server Safe? New OpenSSH Vulnerabilities Exposed

Date of Publication

February 19, 2025

Admiralty Code

A1

TA Number

TA2025050







Summary

First Seen: January 31, 2025

Affected Product: OpenSSH Client and Server

Impact: Two critical vulnerabilities, CVE-2025-26465 and CVE-2025-26466, have been identified in OpenSSH, exposing systems to security risks. CVE-2025-26465 allows attackers to exploit the 'VerifyHostKey' DNS option for machine-in-the-middle (MitM) attacks, leading to credential theft. CVE-2025-26466, is a pre-authentication DoS vulnerability that enables attackers to overwhelm SSH servers, causing service disruption. Keeping OpenSSH updated and properly configured is critical to mitigating these risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-26465	OpenSSH VerifyHostKeyDNS Authentication Bypass Vulnerability	OpenSSH Server			
CVE-2025-26466	OpenSSH Pre-Authentication Denial-of-Service (DoS) Vulnerability	OpenSSH Client and Server			

Vulnerability Details

#1

Two critical vulnerabilities have been identified in OpenSSH, a suite of secure networking utilities based on the Secure Shell (SSH) protocol. The first vulnerability, CVE-2025-26465, affects the OpenSSH client in versions 6.8p1 through 9.9p1 and is linked to the VerifyHostKeyDNS option, which verifies SSH host keys via DNS. When enabled, an attacker positioned between the client and the server can exploit this feature to impersonate a legitimate SSH server, creating a machine-in-the-middle (MitM) attack.

#2

The root cause of this flaw dates back to December 2014, when the affected code was introduced. Due to improper validation of DNS responses, an attacker can forge DNS records and trick the SSH client into accepting an unauthorized host key, potentially leading to credential theft, unauthorized access, or session hijacking.

#3

CVE-2025-26466 is a pre-authentication denial-of-service (DoS) vulnerability that affects both the OpenSSH client and server, specifically versions 9.5p1 through 9.9p1. This flaw allows remote attackers to trigger excessive CPU and memory consumption, leading to service disruption. Since it can be exploited before authentication, it poses a high risk to publicly accessible SSH servers.

#4

The vulnerability originated in August 2023, when changes to the authentication process introduced a flaw that enabled attackers to overwhelm the SSH service with a flood of unauthenticated connection attempts. As a result, an attacker can render the SSH server unresponsive, preventing legitimate users from accessing it. This type of attack can be part of a broader cyber threat campaign, such as disrupting infrastructure or preparing for a more sophisticated intrusion.

#5

As of now, there are no public reports of active exploitation of CVE-2025-26465 or CVE-2025-26466 by threat actors. However, proof-of-concept exploits for both vulnerabilities have been published, it is likely that exploitation efforts by various threat actors will increase. Both vulnerabilities highlight the critical importance of keeping OpenSSH updated and properly configured.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-26465	OpenSSH versions 6.8p1 to 9.9p1	cpe:2.3:a:openssh:openssh:*.~*~*~*~*~*~*~*	
CVE-2025-26466	OpenSSH versions 9.5p1 to 9.9p1	cpe:2.3:a:openssh:openssh:*.~*~*~*~*~*~*~*	

Recommendations



Upgrade OpenSSH Immediately: Organizations should upgrade OpenSSH to version 9.9p2 or later, as this release addresses both vulnerabilities. Keeping OpenSSH updated is essential for minimizing exposure to security risks, and administrators should establish a routine process for applying security patches promptly.



Secure SSH Host Key Verification: Administrators should disable the VerifyHostKeyDNS option unless absolutely necessary, as it can be exploited for man-in-the-middle (MitM) attacks. To strengthen authentication, organizations should use SSH certificates instead of relying on static host keys and manually verify host keys before establishing SSH connections to prevent unauthorized access.



Server-Side Mitigation: Enforce connection limits by configuring LoginGraceTime to reduce the time unauthenticated users can hold a connection open and adjusting MaxStartups to limit concurrent unauthenticated connections. Using PerSourcePenalties can slow down repeated failed attempts from the same source. Firewalls should restrict SSH access to trusted IP ranges and block excessive connection attempts.



Adopt General Security Best Practices: Organizations should enforce key-based authentication instead of password-based logins, enable multi-factor authentication (MFA) for additional security, and monitor SSH logs for unusual activity. Deploying intrusion prevention systems (IPS) can help detect and block potential SSH-based attacks. Implementing strict access controls and monitoring SSH traffic will further strengthen overall system security.



Potential MITRE ATT&CK TTPs

<u>TA0042</u> Resource Development	<u>TA0040</u> Impact	<u>TA0001</u> Initial Access	<u>TA0008</u> Lateral Movement
<u>TA0006</u> Credential Access	<u>T1588</u> Obtain Capabilities	<u>T1588.005</u> Exploits	<u>T1190</u> Exploit Public-Facing Application
<u>T1563</u> Remote Service Session Hijacking	<u>T1212</u> Exploitation for Credential Access	<u>T1499</u> Endpoint Denial of Service	<u>T1588.006</u> Vulnerabilities

Patch Details

Upgrade OpenSSH to the latest version 9.9p2 or later

Link:

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

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

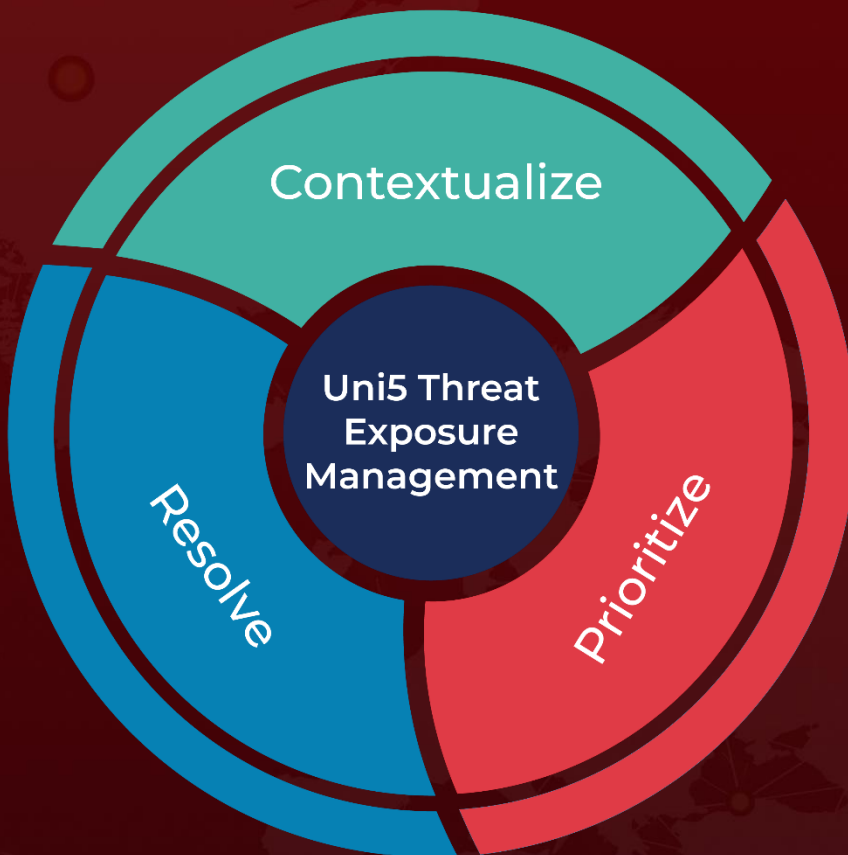
References

<https://blog.qualys.com/vulnerabilities-threat-research/2025/02/18/qualys-tru-discovers-two-vulnerabilities-in-openssh-cve-2025-26465-cve-2025-26466>

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

February 19, 2025 • 7:30 AM

© 2025 All Rights are Reserved by Hive Pro



More at www.hivepro.com