NEWSFLASH

Unmasking CVE-2024-6387: The Critical OpenSSH Flaw Exposing Servers to Remote Attacks

NANGIA & CO LLP

CVE-2024-6387 is a critical security vulnerability identified in the OpenSSH server (sshd). This vulnerability, classified as a Remote Code Execution (RCE) flaw, enables unauthenticated attackers to execute arbitrary code on affected systems. The exploit takes advantage of a previously unknown weakness in the sshd service, allowing remote attackers to gain full control over the target server without requiring valid authentication credentials. The discovery of this vulnerability highlights the ongoing need for vigilance and timely patching in maintaining the security of critical network services.

This advisory outlines the nature of these vulnerabilities, the affected products, and provides guidance on mitigation strategies to safeguard against potential attacks.

NANGIA & CO LLP

What is Remote Unauthenticated Code Execution Vulnerability in OpenSSH server?

A security regression (CVE-2024-6387) was found in OpenSSH's server (sshd). This issue arises from a race condition that causes sshd to handle certain signals unsafely. A remote attacker, without authentication, might exploit this by failing to authenticate within a specified time frame.

The Qualys Threat Research Unit (TRU) discovered an unauthenticated Remote Code Execution (RCE) vulnerability in OpenSSH's server (sshd) on glibc-based Linux systems. This marks the first OpenSSH vulnerability in nearly twenty years and allows an unauthenticated RCE that provides full root access. The vulnerability affects the default configuration and requires no user interaction, representing a significant exploit risk.

What is affected?

OpenSSH versions earlier than 4.4p1 are vulnerable to this signal handler race condition unless they are patched for CVE-2006-5051 and CVE-2008-4109.

Versions from 4.4p1 up to, but not including, 8.5p1 are not vulnerable due to a transformative patch for CVE-2006-5051, which made a previously unsafe function secure.

Versions from 8.5p1 up to, but not including, 9.8p1 are vulnerable due to the accidental removal of a critical component in a function.

OpenBSD systems

What is the Risk?

Remote Code Execution (RCE) vulnerabilities represent a critical security risk, enabling malicious actors to run arbitrary code on affected systems. This type of vulnerability can result in a complete takeover of the system, granting attackers the ability to access sensitive data without authorization and disrupt essential operations significantly. The potential for installing malicious software, elevating access privileges, and spreading infections across interconnected networks amplifies the threat, leading to extensive and possibly irreparable damage. The repercussions of such vulnerabilities are profound, encompassing data breaches, which compromise confidential information, and service interruptions that can halt business operations.

How to check if you are running vulnerable version?

Here are a few steps to follow check the running version of SSH in system.

Step 1: Linux/macOS Command Line: Open terminal. > Type: ssh -V > Press Enter.

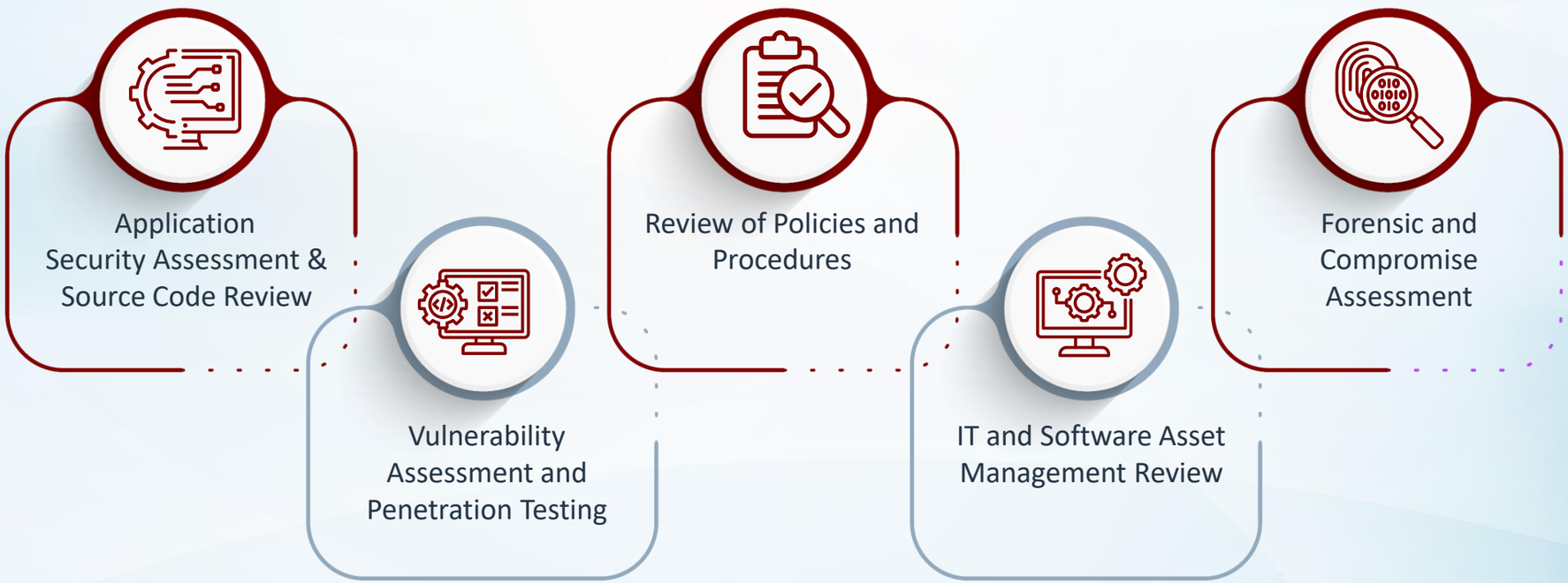
Step 2: Windows: Navigate to Settings > Apps > Optional Features > Check installed OpenSSH version.

How do you protect yourself?

Some of the steps that can be undertaken to protect the organization's infrastructure are:

1. Apply all OpenSSH patches: Apply available patches for OpenSSH (if sshd cannot be updated there is a fix by changing a value in the configuration file, but it does make it vulnerable to DOS).
2. Lock down access control: Limit SSH access via tcp/22 through network-based controls to minimize attack risks
3. Apply segmentation: Divide networks to restrict unauthorized access to the OpenSSH server.
4. Edit your SSH configuration (/etc/ssh/sshd_config) and set PermitRootLogin no.
5. Regular security audits and penetration testing are necessary to identify and mitigate vulnerabilities.
6. Set up a bastion host to act as a gateway for SSH access, reducing the attack surface and centralizing logging and monitoring.
7. Regularly rotate SSH keys and ensure they have strong passphrases.
8. Regularly monitor logs for suspicious activities using tools like fail2ban or SIEM systems like Logpoint SIEM. Deploy an IDS such as Snort or OSSEC to detect and respond to real-time suspicious activities.

How can Nangia & Co LLP Help



NOIDA
(Delhi NCR - Corporate Office) A-109, Sector - 136, Noida - 201304, India
T: +91 120 2598000

DELHI
(Registered Office) B-27, Soami Nagar, New Delhi - 110017, India T: +91 120 2598000

GURUGRAM
001-005, Emaar Digital Greens Tower-A 10th Floor, Golf Course Extension Road, Sector 61, Gurgaon-122102
T: +91 0124 430 1551

MUMBAI
4th Floor, Iconic Tower, URMI Estate, Ganpat Rao Kadam Marg, Lower Parel, Mumbai - 400013, India
T : +91 22 4474 3400

CHENNAI
Prestige Palladium Bayan,
Level 5, 129-140, Greams Road, Thousand Lights, Chennai - 600006 T: +91 44 46549201

BENGALURU
Prestige Obelisk, Level 4, No 3 Kasturba Road, Bengaluru - 560 001, Karnataka, India
T: +91 80 2248 4555

PUNE
3rd Floor, Park Plaza, CTS 1085, Ganeshkhind Road, Next to Pune Central Mall, Shivajinagar, Pune - 411005, India

DEHRADUN
1st Floor, "IDA" 46 E.C. Road, Dehradun - 248001, Uttarakhand, India T: +91 135 271 6300

www.nangia.com | query@nangia.com

Follow us at:

NANGIA & CO LLP