Vulnerability Discovery Results

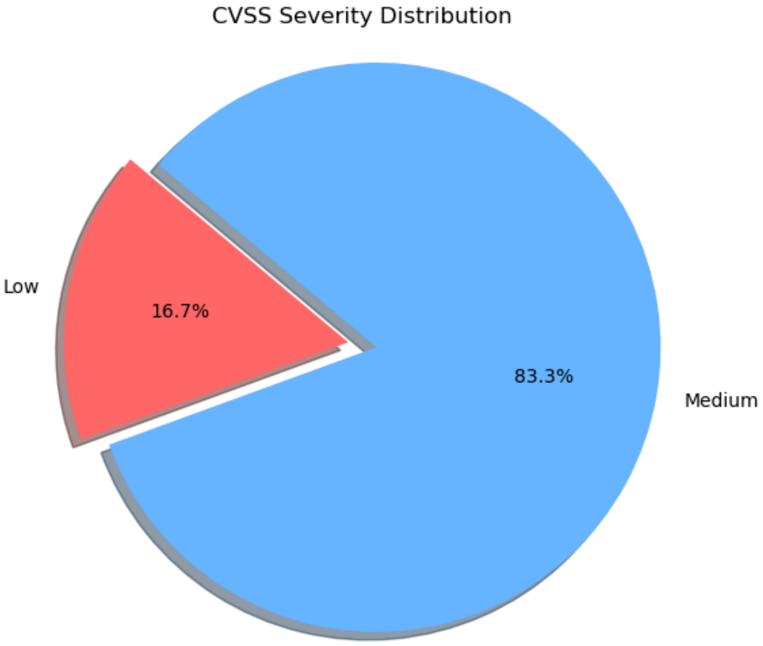
Friday 5th July, 2024

10:16

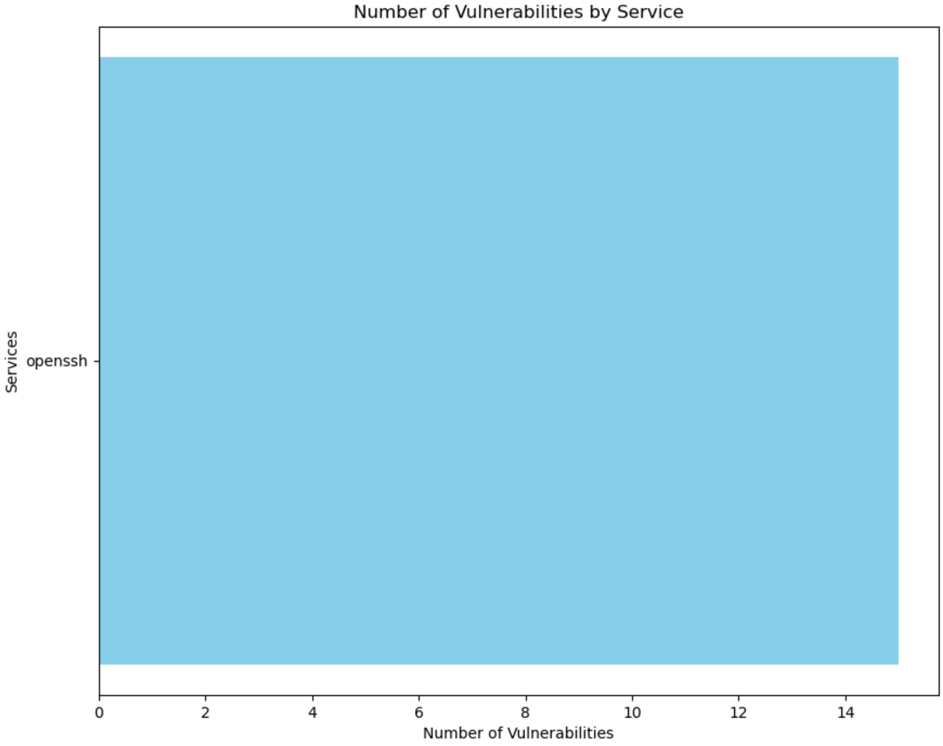
(UTC+2, PARIS)

Company Name	First Name	Last Name
JD	**John**	**Doe**

Name	OS Name	OS SP
linuxt5	**Linux**	**3.14.x**



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

Details

1.1 CVE-2020-15778

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of “anomalous argument transfers” because that could “stand a great chance of breaking existing workflows.”

CVSS: 6.8

1.2 CVE-2019-6111

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).

CVSS: 5.8

1.3 CVE-2017-15906

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

CVSS: 5.0

1.4 CVE-2018-15473

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

CVSS: 5.0

1.5 CVE-2018-15919

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states ‘We understand that the OpenSSH developers do not want to treat such a username enumeration (or “oracle”) as a vulnerability.’

CVSS: 5.0

1.6 CVE-2021-41617

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

CVSS: 4.4

1.7 CVE-2020-14145

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

CVSS: 4.3

1.8 CVE-2016-20012

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

CVSS: 4.3

1.9 CVE-2019-6109

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.

CVSS: 4.0

1.10 CVE-2019-6110

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

CVSS: 4.0

1.11 CVE-2018-20685

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:::::::*

Summary: In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.

CVSS: 2.6

1.12 CVE-2021-36368

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:::::::*

Summary: An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

CVSS: 2.6

1.13 CVE-2023-38408

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:::::::*

Summary: The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

CVSS: N/A

1.14 CVE-2023-48795

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:::::::*

Summary: The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

CVSS: N/A

1.15 CVE-2023-51385

!–> CVE for cpe:2.3:a:openbsd:openssh:7.4:*:*:*:*:*:*:*

Summary: In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.

CVSS: N/A