Vulnerability Discovery Results

Monday 8th July, 2024

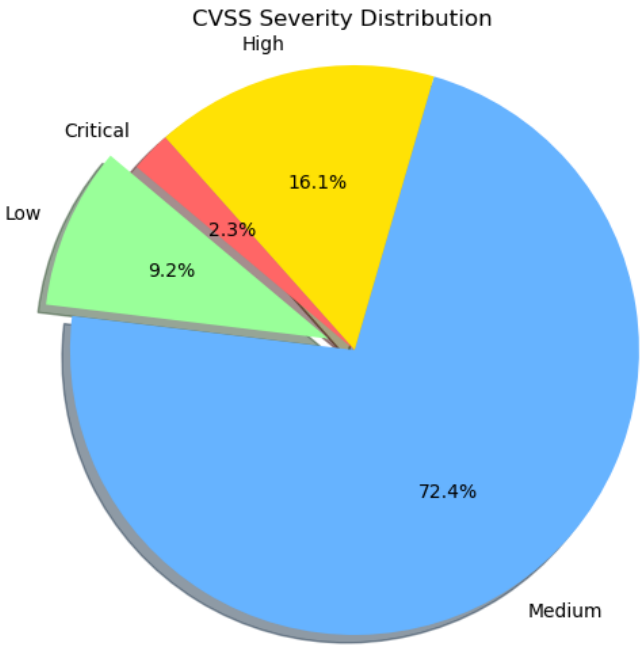
17:55

(UTC+2, PARIS)

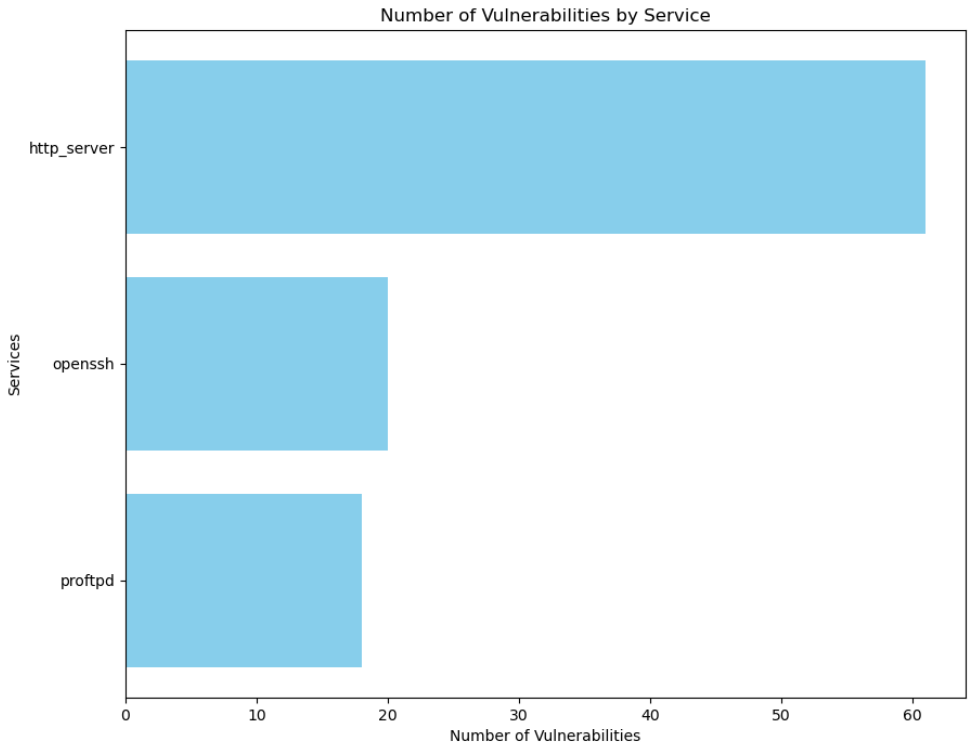
Company Name	First Name	Last Name
VirtualBox	**Abagail**	**Blaik**

Name	OS Name	OS SP
SecNo	**Linux**	**16.04**

CVE	Critical Severity
CVE-2010-4221	10.0
CVE-2011-4130	9.0



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

Details

1.1 CVE-2010-4221

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: Multiple stack-based buffer overflows in the pr_netio_telnet_gets function in netio.c in ProFTPD before 1.3.3c allow remote attackers to execute arbitrary code via vectors involving a TELNET IAC escape character to a (1) FTP or (2) FTPS server.

CVSS: 10.0

1.2 CVE-2011-4130

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: Use-after-free vulnerability in the Response API in ProFTPD before 1.3.3g allows remote authenticated users to execute arbitrary code via vectors involving an error that occurs after an FTP data transfer.

CVSS: 9.0

1.3 CVE-2019-12815

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.

CVSS: 7.5

1.4 CVE-2010-3867

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: Multiple directory traversal vulnerabilities in the mod_site_misc module in ProFTPD before 1.3.3c allow remote authenticated users to create directories, delete directories, create symlinks, and modify file timestamps via directory traversal sequences in a (1) SITE MKDIR, (2) SITE RMDIR, (3) SITE SYMLINK, or (4) SITE UTIME command.

CVSS: 7.1

1.5 CVE-2010-4652

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: Heap-based buffer overflow in the sql_prepare_where function (contrib/mod_sql.c) in ProFTPD before 1.3.3d, when mod_sql is enabled, allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted username containing substitution tags, which are not properly handled during construction of an SQL query.

CVSS: 6.8

1.6 CVE-2011-1137

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: Integer overflow in the mod_sftp (aka SFTP) module in ProFTPD 1.3.3d and earlier allows remote attackers to cause a denial of service (memory consumption leading to OOM kill) via a malformed SSH message.

CVSS: 5.0

1.7 CVE-2016-3125

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: The mod_tls module in ProFTPD before 1.3.5b and 1.3.6 before 1.3.6rc2 does not properly handle the TLSDHParamFile directive, which might cause a weaker than intended Diffie-Hellman (DH) key to be used and consequently allow attackers to have unspecified impact via unknown vectors.

CVSS: 5.0

1.8 CVE-2019-18217

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: ProFTPD before 1.3.6b and 1.3.7rc before 1.3.7rc2 allows remote unauthenticated denial-of-service due to incorrect handling of overly long commands because main.c in a child process enters an infinite loop.

CVSS: 5.0

1.9 CVE-2019-19270

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: An issue was discovered in tls_verify_crl in ProFTPD through 1.3.6b. Failure to check for the appropriate field of a CRL entry (checking twice for subject, rather than once for subject and once for issuer) prevents some valid CRLs from being taken into account, and can allow clients whose certificates have been revoked to proceed with a connection to the server.

CVSS: 5.0

1.10 CVE-2019-19271

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: An issue was discovered in tls_verify_crl in ProFTPD before 1.3.6. A wrong iteration variable, used when checking a client certificate against CRL entries (installed by a system administrator), can cause some CRL entries to be ignored, and can allow clients whose certificates have been revoked to proceed with a connection to the server.

CVSS: 5.0

1.11 CVE-2019-19272

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: An issue was discovered in tls_verify_crl in ProFTPD before 1.3.6. Direct dereference of a NULL pointer (a variable initialized to NULL) leads to a crash when validating the certificate of a client connecting to the server in a TLS client/server mutual-authentication setup.

CVSS: 5.0

1.12 CVE-2020-9272

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: ProFTPD 1.3.7 has an out-of-bounds (OOB) read vulnerability in mod_cap via the cap_text.c cap_to_text function.

CVSS: 5.0

1.13 CVE-2019-19269

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: An issue was discovered in tls_verify_crl in ProFTPD through 1.3.6b. A dereference of a NULL pointer may occur. This pointer is returned by the OpenSSL sk_X509_REVOKED_value() function when encountering an empty CRL installed by a system administrator. The dereference occurs when validating the certificate of a client connecting to the server in a TLS client/server mutual-authentication setup.

CVSS: 4.0

1.14 CVE-2017-7418

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: ProFTPD before 1.3.5e and 1.3.6 before 1.3.6rc5 controls whether the home directory of a user could contain a symbolic link through the AllowChrootSymlinks configuration option, but checks only the last path component when enforcing AllowChrootSymlinks. Attackers with local access could bypass the AllowChrootSymlinks control by replacing a path component (other than the last one) with a symbolic link. The threat model includes an attacker who is not granted full filesystem access by a hosting provider, but can reconfigure the home directory of an FTP user.

CVSS: 2.1

1.15 CVE-2012-6095

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: ProFTPD before 1.3.5rc1, when using the UserOwner directive, allows local users to modify the ownership of arbitrary files via a race condition and a symlink attack on the (1) MKD or (2) XMKD commands.

CVSS: 1.2

1.16 CVE-2021-46854

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: mod_radius in ProFTPD before 1.3.7c allows memory disclosure to RADIUS servers because it copies blocks of 16 characters.

CVSS: N/A

1.17 CVE-2023-48795

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

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

1.18 CVE-2023-51713

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.3:b:::::

Summary: make_ftp_cmd in main.c in ProFTPD before 1.3.8a has a one-byte out-of-bounds read, and daemon crash, because of mishandling of quote/backslash semantics.

CVSS: N/A

1.19 CVE-2016-10009

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

Summary: Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.

CVSS: 7.5

1.20 CVE-2016-10012

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

Summary: The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced

by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.

CVSS: 7.2

1.21 CVE-2016-10010

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

Summary: sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.

CVSS: 6.9

1.22 CVE-2020-15778

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.23 CVE-2019-6111

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.24 CVE-2017-15906

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.25 CVE-2016-10708

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

Summary: sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

CVSS: 5.0

1.26 CVE-2018-15473

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.27 CVE-2018-15919

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.28 CVE-2021-41617

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.29 CVE-2020-14145

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.30 CVE-2016-20012

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.31 CVE-2019-6109

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.32 CVE-2019-6110

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.33 CVE-2018-20685

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.34 CVE-2021-36368

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.35 CVE-2016-10011

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

Summary: authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.

CVSS: 2.1

1.36 CVE-2023-38408

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.37 CVE-2023-48795

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.38 CVE-2023-51385

!–> CVE for cpe:2.3:a:openbsd:openssh:7.2:p2:::::

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

1.39 CVE-2017-3167

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

CVSS: 7.5

1.40 CVE-2017-3169

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

CVSS: 7.5

1.41 CVE-2017-7679

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

CVSS: 7.5

1.42 CVE-2021-26691

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow

CVSS: 7.5

1.43 CVE-2021-39275

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 7.5

1.44 CVE-2021-44790

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerabilty though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

CVSS: 7.5

1.45 CVE-2022-22720

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling

CVSS: 7.5

1.46 CVE-2022-23943

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

CVSS: 7.5

1.47 CVE-2022-31813

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.

CVSS: 7.5

1.48 CVE-2019-0211

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.

CVSS: 7.2

1.49 CVE-2016-5387

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.

CVSS: 6.8

1.50 CVE-2017-15715

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd 2.4.0 to 2.4.29, the expression specified in could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

CVSS: 6.8

1.51 CVE-2018-1312

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

CVSS: 6.8

1.52 CVE-2020-35452

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow

CVSS: 6.8

1.53 CVE-2021-40438

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 6.8

1.54 CVE-2017-9788

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

CVSS: 6.4

1.55 CVE-2019-10082

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4.18-2.4.39, using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.

CVSS: 6.4

1.56 CVE-2021-44224

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).

CVSS: 6.4

1.57 CVE-2022-28615

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

CVSS: 6.4

1.58 CVE-2019-0217

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.

CVSS: 6.0

1.59 CVE-2019-10098

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.

CVSS: 5.8

1.60 CVE-2020-1927

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.

CVSS: 5.8

1.61 CVE-2022-22721

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVSS: 5.8

1.62 CVE-2016-4979

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: The Apache HTTP Server 2.4.18 through 2.4.20, when mod_http2 and mod_ssl are enabled, does not properly recognize the "SSLVerifyClient require" directive for HTTP/2 request authorization, which allows remote attackers to bypass intended access restrictions by leveraging the ability to send multiple requests over a single connection and aborting a renegotiation.

CVSS: 5.0

1.63 CVE-2016-8740

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.

CVSS: 5.0

1.64 CVE-2016-8743

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVSS: 5.0

1.65 CVE-2017-9798

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through

2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.

CVSS: 5.0

1.66 CVE-2017-15710

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

CVSS: 5.0

1.67 CVE-2018-1303

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.

CVSS: 5.0

1.68 CVE-2018-1333

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

CVSS: 5.0

1.69 CVE-2018-17189

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.

CVSS: 5.0

1.70 CVE-2018-17199

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.

CVSS: 5.0

1.71 CVE-2019-0220

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

CVSS: 5.0

1.72 CVE-2019-0196

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.

CVSS: 5.0

1.73 CVE-2020-1934

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.

CVSS: 5.0

1.74 CVE-2019-17567

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.

CVSS: 5.0

1.75 CVE-2021-26690

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service

CVSS: 5.0

1.76 CVE-2021-33193

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.

CVSS: 5.0

1.77 CVE-2021-34798

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.

CVSS: 5.0

1.78 CVE-2022-22719

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVSS: 5.0

1.79 CVE-2022-26377

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.

CVSS: 5.0

1.80 CVE-2022-28330

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.

CVSS: 5.0

1.81 CVE-2022-28614

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input

using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.

CVSS: 5.0

1.82 CVE-2022-29404

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.

CVSS: 5.0

1.83 CVE-2022-30556

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.

CVSS: 5.0

1.84 CVE-2016-1546

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: The Apache HTTP Server 2.4.17 and 2.4.18, when mod_http2 is enabled, does not limit the number of simultaneous stream workers for a single HTTP/2 connection, which allows remote attackers to cause a denial of service (stream-processing outage) via modified flow-control windows.

CVSS: 4.3

1.85 CVE-2018-1301

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

CVSS: 4.3

1.86 CVE-2018-1302

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

CVSS: 4.3

1.87 CVE-2016-4975

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).

CVSS: 4.3

1.88 CVE-2018-11763

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.

CVSS: 4.3

1.89 CVE-2019-10092

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.

CVSS: 4.3

1.90 CVE-2020-11985

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: IP address spoofing when proxying using mod_remoteip and mod_rewrite For configurations using proxying with mod_remoteip and certain mod_rewrite rules, an attacker could spoof their IP address for logging and PHP scripts. Note this issue was fixed in Apache HTTP Server 2.4.24 but was retrospectively allocated a low severity CVE in 2020.

CVSS: 4.3

1.91 CVE-2018-1283

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

CVSS: 3.5

1.92 CVE-2016-8612

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

CVSS: 3.3

1.93 CVE-2020-13938

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows

CVSS: 2.1

1.94 CVE-2006-20001

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash.

This issue affects Apache HTTP Server 2.4.54 and earlier.

CVSS: N/A

1.95 CVE-2022-36760

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions.

CVSS: N/A

1.96 CVE-2022-37436

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client.

CVSS: N/A

1.97 CVE-2023-25690

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack.

Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion

of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like:

RewriteEngine on RewriteRule "^/here/(.*)" "http://example.com:8080/elsewhere?$1"; [P] ProxyPassReverse /here/ http://example.com:8080/

Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Users are recommended to update to at least version 2.4.56 of Apache HTTP Server.

CVSS: N/A

1.98 CVE-2023-31122

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.

CVSS: N/A

1.99 CVE-2023-45802

!–> CVE for cpe:2.3:a:apache:http_server:2.4.18:::::*

Summary: When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.

This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out.

Users are recommended to upgrade to version 2.4.58, which fixes the issue.

CVSS: N/A