Vulnerability Discovery Results

Saturday 6th July, 2024

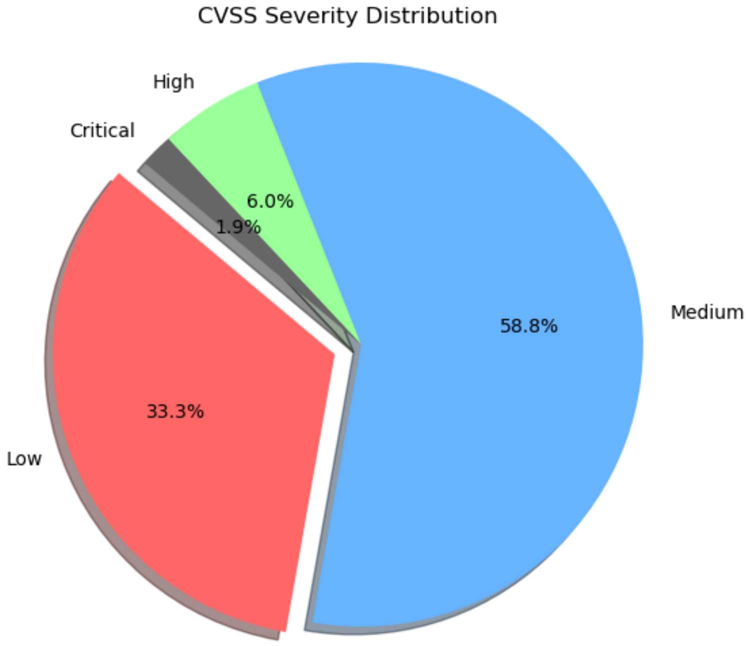
18:27

(UTC+2, PARIS)

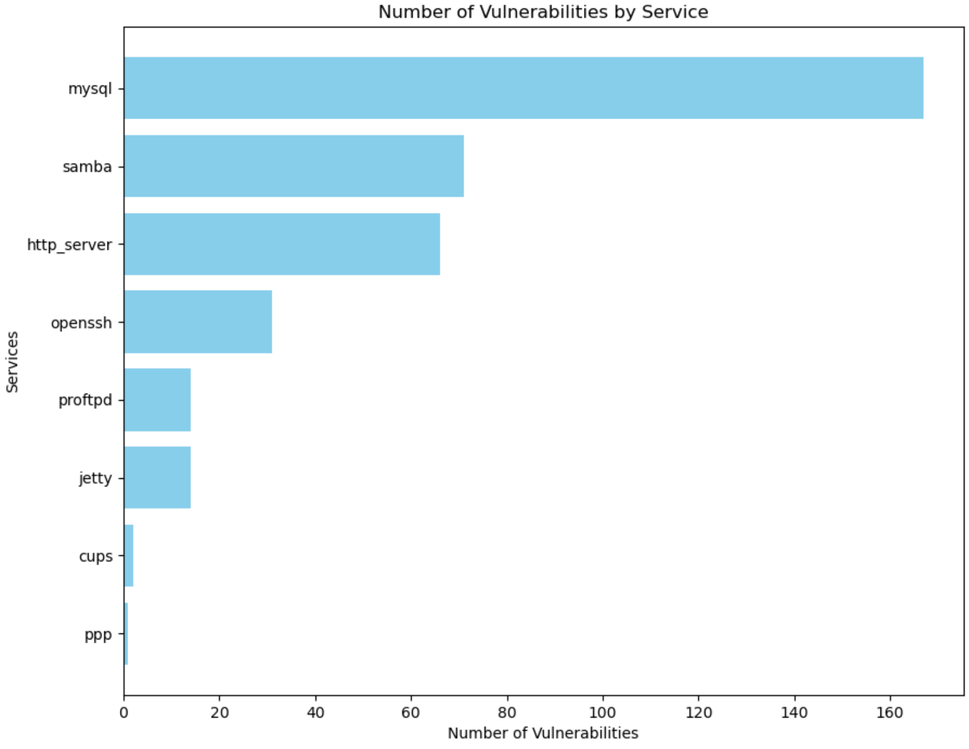
Company Name	First Name	Last Name
Wikipedia	Deloria	Brandham

Name	OS Name	OS SP
metalink4	Linux	14.04.6

CVE	Critical Severity
CVE-2015-3306	10.0
CVE-2017-7494	10.0
CVE-2020-1472	9.3
CVE-2020-17049	9.0
CVE-2020-25719	9.0
CVE-2021-44142	9.0
CVE-2015-1158	10.0



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

Details

1.1 CVE-2015-3306

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

Summary: The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

CVSS: 10.0

1.2 CVE-2019-12815

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.3 CVE-2016-3125

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.4 CVE-2019-18217

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.5 CVE-2019-19270

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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once for issuer) prevents some valid CRLs from being taken into account, and can allow clients whose certificates have been revoked to proceed with a connection to the server.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

1.6 CVE-2019-19271

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.7 CVE-2019-19272

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.8 CVE-2020-9272

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.9 CVE-2013-4359

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

Summary: Integer overflow in kbdint.c in mod_sftp in ProFTPD 1.3.4d and 1.3.5r3 allows remote attackers to cause a denial of service (memory consumption) via a large response count value in an authentication request, which triggers a large memory allocation.

CVSS: 5.0

1.10 CVE-2019-19269

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.11 CVE-2017-7418

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:::::::*

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

1.12 CVE-2021-46854

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:*:*:*:*:*:*:*

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

1.13 CVE-2023-48795

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:*:*:*:*:*:*:*

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

1.14 CVE-2023-51713

!–> CVE for cpe:2.3:a:proftpd:proftpd:1.3.5:*:*:*:*:*:*:*

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

1.15 CVE-2015-5600

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

Summary: The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

CVSS: 8.5

1.16 CVE-2016-6515

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

Summary: The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

CVSS: 7.8

1.17 CVE-2016-10009

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.18 CVE-2016-1908

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

Summary: The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.

CVSS: 7.5

1.19 CVE-2015-8325

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

Summary: The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.

CVSS: 7.2

1.20 CVE-2016-10012

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

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-2015-6564

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

Summary: Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.

CVSS: 6.9

1.22 CVE-2016-10010

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

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

1.23 CVE-2020-15778

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

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

1.24 CVE-2019-6111

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

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

1.25 CVE-2016-3115

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::::

Summary: Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.

CVSS: 5.5

1.26 CVE-2017-15906

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::::

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

1.27 CVE-2016-10708

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::::

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

1.28 CVE-2018-15473

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::::

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

1.29 CVE-2018-15919

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::::

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

1.30 CVE-2016-0778

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::::

Summary: The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

CVSS: 4.6

1.31 CVE-2021-41617

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.32 CVE-2015-5352

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

Summary: The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.

CVSS: 4.3

1.33 CVE-2016-6210

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

Summary: sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

CVSS: 4.3

1.34 CVE-2020-14145

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.35 CVE-2016-20012

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.36 CVE-2016-0777

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

Summary: The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

CVSS: 4.0

1.37 CVE-2019-6109

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.38 CVE-2019-6110

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.39 CVE-2018-20685

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.40 CVE-2021-36368

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:*:*:*:*:*:*

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

1.41 CVE-2016-10011

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

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

1.42 CVE-2015-6563

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

Summary: The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.

CVSS: 1.9

1.43 CVE-2023-38408

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

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

1.44 CVE-2023-48795

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1:::::

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

1.45 CVE-2023-51385

!–> CVE for cpe:2.3:a:openbsd:openssh:6.6:p1::::::

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

1.46 CVE-2017-3167

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.47 CVE-2017-7679

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.48 CVE-2021-26691

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.49 CVE-2021-39275

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.50 CVE-2021-44790

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.51 CVE-2022-22720

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.52 CVE-2022-23943

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.53 CVE-2022-31813

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.54 CVE-2014-0226

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVSS: 6.8

1.55 CVE-2016-5387

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.56 CVE-2017-15715

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.57 CVE-2018-1312

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.58 CVE-2020-35452

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.59 CVE-2021-40438

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.60 CVE-2017-9788

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.61 CVE-2021-44224

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.62 CVE-2022-28615

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.63 CVE-2019-0217

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.64 CVE-2019-10098

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.65 CVE-2020-1927

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.66 CVE-2022-22721

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.67 CVE-2013-6438

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

CVSS: 5.0

1.68 CVE-2014-0098

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

CVSS: 5.0

1.69 CVE-2013-5704

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass “RequestHeader unset” directives by placing a header in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states “this is not a security issue in httpd as such.”

CVSS: 5.0

1.70 CVE-2014-0231

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

CVSS: 5.0

1.71 CVE-2014-3523

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

CVSS: 5.0

1.72 CVE-2014-3581

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.

CVSS: 5.0

1.73 CVE-2015-0228

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.

CVSS: 5.0

1.74 CVE-2015-3183

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.

CVSS: 5.0

1.75 CVE-2015-3184

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.

CVSS: 5.0

1.76 CVE-2016-0736

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

CVSS: 5.0

1.77 CVE-2016-2161

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

CVSS: 5.0

1.78 CVE-2016-8743

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.79 CVE-2017-9798

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.80 CVE-2017-15710

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.81 CVE-2018-1303

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.82 CVE-2018-17199

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.83 CVE-2019-0220

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.84 CVE-2020-1934

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.85 CVE-2019-17567

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.86 CVE-2021-26690

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.87 CVE-2021-34798

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.88 CVE-2022-22719

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.89 CVE-2022-26377

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.90 CVE-2022-28330

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.91 CVE-2022-28614

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.92 CVE-2022-29404

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.93 CVE-2022-30556

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.94 CVE-2014-0117

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

CVSS: 4.3

1.95 CVE-2014-0118

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

CVSS: 4.3

1.96 CVE-2014-8109

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

CVSS: 4.3

1.97 CVE-2015-3185

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

Summary: The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVSS: 4.3

1.98 CVE-2018-1301

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.99 CVE-2018-1302

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.100 CVE-2016-4975

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:::::::*

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

1.101 CVE-2019-10092

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.102 CVE-2020-11985

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.103 CVE-2018-1283

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.104 CVE-2016-8612

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.105 CVE-2020-13938

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

CVSS: 2.1

1.106 CVE-2006-20001

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.107 CVE-2022-36760

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.108 CVE-2022-37436

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.109 CVE-2023-25690

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.110 CVE-2023-31122

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.111 CVE-2023-45802

!–> CVE for cpe:2.3:a:apache:http_server:2.4.7:*:*:*:*:*:*:*

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

1.112 CVE-2017-7494

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

CVSS: 10.0

1.113 CVE-2020-1472

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC). An attacker who successfully exploited the vulnerability could run a specially crafted application on a device on the network. To exploit the vulnerability, an unauthenticated attacker would be required to use MS-NRPC to connect to a domain controller to obtain domain administrator access. Microsoft is addressing the vulnerability in a phased two-part rollout. These updates address the vulnerability by modifying how Netlogon handles the usage of Netlogon secure channels. For guidelines on how to manage the changes required for this vulnerability and more information on the phased rollout, see How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 (updated September 28, 2020). When the second phase of Windows updates become available in Q1 2021, customers will be notified via a revision to this security vulnerability. If you wish to be notified when these updates are released, we recommend that you register for the security notifications mailer to be alerted of content changes to this advisory. See Microsoft Technical Security Notifications.

CVSS: 9.3

1.114 CVE-2020-17049

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary:

A security feature bypass vulnerability exists in the way Key Distribution Center (KDC) determines if a service ticket can be used for delegation via Kerberos Constrained Delegation (KCD).

To exploit the vulnerability, a compromised service that is configured to use KCD could tamper with a service ticket that is not valid for delegation to force the KDC to accept it.

The update addresses this vulnerability by changing how the KDC validates service tickets used with KCD.

CVSS: 9.0

1.115 CVE-2020-25719

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in the way Samba, as an Active Directory Domain Controller, implemented Kerberos name-based authentication. The Samba AD DC, could become confused about the user a ticket represents if it did not strictly require a Kerberos PAC and always use the SIDs found within. The result could include total domain compromise.

CVSS: 9.0

1.116 CVE-2021-44142

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.

CVSS: 9.0

1.117 CVE-2020-25717

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.

CVSS: 8.5

1.118 CVE-2020-10745

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability.

CVSS: 7.8

1.119 CVE-2017-14746

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.

CVSS: 7.5

1.120 CVE-2017-9461

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: smbd in Samba before 4.4.10 and 4.5.x before 4.5.6 has a denial of service vulnerability (fd_open_atomic infinite loop with high CPU usage and memory consumption) due to wrongly handling dangling symlinks.

CVSS: 6.8

1.121 CVE-2017-11103

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.

CVSS: 6.8

1.122 CVE-2018-1057

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: On a Samba 4 AD DC the LDAP server in all versions of Samba from 4.0.0 onwards incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).

CVSS: 6.5

1.123 CVE-2018-10858

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.

CVSS: 6.5

1.124 CVE-2016-2123

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in samba versions 4.0.0 to 4.5.2. The Samba routine ndr_pull_dnsp_name contains an integer wrap problem, leading to an attacker-controlled memory overwrite. ndr_pull_dnsp_name parses data from the Samba Active Directory ldb database. Any user who can write to the dnsRecord attribute over LDAP can trigger this memory corruption. By default, all authenticated LDAP users can write to the dnsRecord attribute on new DNS objects. This makes the defect a remote privilege escalation.

CVSS: 6.5

1.125 CVE-2020-25718

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in the way samba, as an Active Directory Domain Controller, is able to support an RODC (read-only domain controller). This would allow an RODC to print administrator tickets.

CVSS: 6.5

1.126 CVE-2020-25722

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: Multiple flaws were found in the way samba AD DC implemented access and conformance checking of stored data. An attacker could use this flaw to cause total domain compromise.

CVSS: 6.5

1.127 CVE-2021-3738

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: In DCE/RPC it is possible to share the handles (cookies for resource state) between multiple connections via a mechanism called 'association groups'. These handles can reference connections to our sam.ldb database. However while the database was correctly shared, the user credentials state was only pointed at, and when one connection within that association group ended, the database would be left pointing at an invalid 'struct session_info'. The most likely outcome here is a crash, but it is possible that the use-after-free could instead allow different user state to be pointed at and this might allow more privileged access.

CVSS: 6.5

1.128 CVE-2019-14870

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the S4U (MS-SFU) Kerberos delegation model includes a feature allowing for a subset of clients to be opted out of constrained delegation in any way, either S4U2Self or regular Kerberos authentication, by forcing all tickets for these clients to be non-forwardable. In AD this is implemented by a user attribute delegation_not_allowed (aka not-delegated), which translates to disallow-forwardable. However the Samba AD DC does not do that for S4U2Self and does set the forwardable flag even if the impersonated client has the not-delegated flag set.

CVSS: 6.4

1.129 CVE-2017-2619

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Samba before versions 4.6.1, 4.5.7 and 4.4.11 are vulnerable to a malicious client using a symlink race to allow access to areas of the server file system not exported under the share definition.

CVSS: 6.0

1.130 CVE-2017-12150

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.

CVSS: 5.8

1.131 CVE-2017-12151

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.

CVSS: 5.8

1.132 CVE-2019-3880

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.

CVSS: 5.5

1.133 CVE-2019-14902

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: There is an issue in all samba 4.11.x versions before 4.11.5, all samba 4.10.x versions before 4.10.12 and all samba 4.9.x versions before 4.9.18, where the removal of the right to create or modify a subtree would not automatically be taken away on all domain controllers.

CVSS: 5.5

1.134 CVE-2017-15275

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.

CVSS: 5.0

1.135 CVE-2020-10704

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found when using samba as an Active Directory Domain Controller. Due to the way samba handles certain requests as an Active Directory Domain Controller LDAP server, an unauthorized user can cause a stack overflow leading to a denial of service. The highest threat from this vulnerability is to system availability. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.

CVSS: 5.0

1.136 CVE-2021-20277

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of-bounds memory write, leading to a crash of the LDAP server process handling the request. The highest threat from this vulnerability is to system availability.

CVSS: 5.0

1.137 CVE-2020-27840

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in samba. Spaces used in a string around a domain name (DN), while supposed to be ignored, can cause invalid DN strings with spaces to instead write a zero-byte into out-of-bounds memory, resulting in a crash. The highest threat from this vulnerability is to system availability.

CVSS: 5.0

1.138 CVE-2021-20254

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.

CVSS: 4.9

1.139 CVE-2017-12163

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.

CVSS: 4.8

1.140 CVE-2019-10218

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.

CVSS: 4.3

1.141 CVE-2016-2124

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.

CVSS: 4.3

1.142 CVE-2016-2126

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: Samba version 4.0.0 up to 4.5.2 is vulnerable to privilege elevation due to incorrect handling of the PAC (Privilege Attribute Certificate) checksum. A remote, authenticated, attacker can cause the winbindd process to crash using a legitimate Kerberos ticket. A local service with access to the winbindd privileged pipe can cause winbindd to cache elevated access permissions.

CVSS: 4.0

1.143 CVE-2018-10919

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.

CVSS: 4.0

1.144 CVE-2018-14629

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.

CVSS: 4.0

1.145 CVE-2018-16841

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.

CVSS: 4.0

1.146 CVE-2018-16851

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.

CVSS: 4.0

1.147 CVE-2019-3824

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in the way an LDAP search expression could crash the shared LDAP server process of a samba AD DC in samba before version 4.10. An authenticated user, having read permissions on the LDAP server, could use this flaw to cause denial of service.

CVSS: 4.0

1.148 CVE-2019-14847

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in samba 4.0.0 before samba 4.9.15 and samba 4.10.x before 4.10.10. An attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.

CVSS: 4.0

1.149 CVE-2020-14383

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not.

CVSS: 4.0

1.150 CVE-2020-14318

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.

CVSS: 4.0

1.151 CVE-2021-3671

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A null pointer de-reference was found in the way samba kerberos server handled missing sname in TGS-REQ (Ticket Granting Server - Request). An authenticated user could use this flaw to crash the samba server.

CVSS: 4.0

1.152 CVE-2019-14861

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: All Samba versions 4.x.x before 4.9.17, 4.10.x before 4.10.11 and 4.11.x before 4.11.3 have an issue, where the (poorly named) dnsserver RPC pipe provides administrative facilities to modify DNS records and zones. Samba, when acting as an AD DC, stores DNS records in LDAP. In AD, the default permissions on the DNS partition allow creation of new records by authenticated users. This is used for example to allow machines to self-register in DNS. If a DNS record was created that case-insensitively matched the name of the zone, the ldb_qsort() and dns_name_compare() routines could be confused into reading memory prior to the list of DNS entries when responding to DnssrvEnumRecords() or DnssrvEnumRecords2() and so following invalid memory as a pointer.

CVSS: 3.5

1.153 CVE-2021-44141

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: All versions of Samba prior to 4.15.5 are vulnerable to a malicious client using a server symlink to determine if a file or directory exists in an area of the server file system not exported under the share definition. SMB1 with unix extensions has to be enabled in order for this attack to succeed.

CVSS: 3.5

1.154 CVE-2018-1050

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: All versions of Samba from 4.0.0 onwards are vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash.

CVSS: 3.3

1.155 CVE-2016-2125

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: It was found that Samba before versions 4.5.3, 4.4.8, 4.3.13 always requested forwardable tickets when using Kerberos authentication. A service to which Samba authenticated using Kerberos could subsequently use the ticket to impersonate Samba to other services or domain users.

CVSS: 3.3

1.156 CVE-2020-14323

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.

CVSS: 2.1

1.157 CVE-2021-43566

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: All versions of Samba prior to 4.13.16 are vulnerable to a malicious client using an SMB1 or NFS race to allow a directory to be created in an area of the server file system not exported under the share definition. Note that SMB1 has to be enabled, or the share also available via NFS in order for this attack to succeed.

CVSS: 1.2

1.158 CVE-2021-20316

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in the way Samba handled file/directory metadata. This flaw allows an authenticated attacker with permissions to read or modify share metadata, to perform this operation outside of the share.

CVSS: N/A

1.159 CVE-2021-3670

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: MaxQueryDuration not honoured in Samba AD DC LDAP

CVSS: N/A

1.160 CVE-2022-2031

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in Samba. The security vulnerability occurs when KDC and the kpasswd service share a single account and set of keys, allowing them to decrypt each other's tickets. A user who has been requested to change their password, can exploit this flaw to obtain and use tickets to other services.

CVSS: N/A

1.161 CVE-2022-32742

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in Samba. Some SMB1 write requests were not correctly range-checked to ensure the client had sent enough data to fulfill the write, allowing server memory contents to be written into the file (or printer) instead of client-supplied data. The client cannot control the area of the server memory written to the file (or printer).

CVSS: N/A

1.162 CVE-2022-32744

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in Samba. The KDC accepts kpasswd requests encrypted with any key known to it. By encrypting forged kpasswd requests with its own key, a user can change other users' passwords, enabling full domain takeover.

CVSS: N/A

1.163 CVE-2022-32746

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A flaw was found in the Samba AD LDAP server. The AD DC database audit logging module can access LDAP message values freed by a preceding database module, resulting in a use-after-free issue. This issue is only possible when modifying certain privileged attributes, such as userAccountControl.

CVSS: N/A

1.164 CVE-2022-0336

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: The Samba AD DC includes checks when adding service principals names (SPNs) to an account to ensure that SPNs do not alias with those already in the database. Some of these checks are able to be bypassed if an account modification re-adds an SPN that was previously present on that account, such as one added when a computer is joined to a domain. An attacker who has the ability to write to an account can exploit this to perform a denial-of-service attack by adding an SPN that matches an existing service. Additionally, an attacker who can intercept traffic can impersonate existing services, resulting in a loss of confidentiality and integrity.

CVSS: N/A

1.165 CVE-2022-1615

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: In Samba, GnuTLS gnutls_rnd() can fail and give predictable random values.

CVSS: N/A

1.166 CVE-2022-32743

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: Samba does not validate the Validated-DNS-Host-Name right for the dNSHostName attribute which could permit unprivileged users to write it.

CVSS: N/A

1.167 CVE-2022-42898

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may lead to remote code execution (in KDC, kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer overflow), and cause a denial of service on other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has “a similar bug.”

CVSS: N/A

1.168 CVE-2022-3437

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A heap-based buffer overflow vulnerability was found in Samba within the GSSAPI unwrap_des() and unwrap_des3() routines of Heimdal. The DES and Triple-DES decryption routines in the Heimdal GSSAPI library allow a length-limited write buffer overflow on malloc() allocated memory when presented with a maliciously small packet. This flaw allows a remote user to send specially crafted malicious data to the application, possibly resulting in a denial of service (DoS) attack.

CVSS: N/A

1.169 CVE-2018-14628

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: An information leak vulnerability was discovered in Samba’s LDAP server. Due to missing access control checks, an authenticated but unprivileged attacker could discover the names and preserved attributes of deleted objects in the LDAP store.

CVSS: N/A

1.170 CVE-2021-20251

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in samba. A race condition in the password lockout code may lead to the risk of brute force attacks being successful if special conditions are met.

CVSS: N/A

1.171 CVE-2022-45141

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: Since the Windows Kerberos RC4-HMAC Elevation of Privilege Vulnerability was disclosed by Microsoft on Nov 8 2022 and per RFC8429 it is assumed that rc4-hmac is weak, Vulnerable Samba Active Directory DCs will issue rc4-hmac encrypted tickets despite the target server supporting better encryption (eg aes256-cts-hmac-sha1-96).

CVSS: N/A

1.172 CVE-2023-0614

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure vi LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC.

CVSS: N/A

1.173 CVE-2023-0922

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: The Samba AD DC administration tool, when operating against a remote LDAP server, will by default send new or reset passwords over a signed-only connection.

CVSS: N/A

1.174 CVE-2023-34966

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: An infinite loop vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial of service condition.

CVSS: N/A

1.175 CVE-2023-34967

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:*:*:*:*:*:*:*

Summary: A Type Confusion vulnerability was found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the mdssvc protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a caller may trigger a crash in talloc_get_size() when talloc detects that the passed-in pointer is not a valid talloc pointer. With an RPC worker process shared among multiple client connections, a malicious client or attacker can trigger a process crash in a shared RPC mdssvc worker process, affecting all other clients this worker serves.

CVSS: N/A

1.176 CVE-2023-34968

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A path disclosure vulnerability was found in Samba. As part of the Spotlight protocol, Samba discloses the server-side absolute path of shares, files, and directories in the results for search queries. This flaw allows a malicious client or an attacker with a targeted RPC request to view the information that is part of the disclosed path.

CVSS: N/A

1.177 CVE-2023-5568

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A heap-based Buffer Overflow flaw was discovered in Samba. It could allow a remote, authenticated attacker to exploit this vulnerability to cause a denial of service.

CVSS: N/A

1.178 CVE-2023-42670

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A flaw was found in Samba. It is susceptible to a vulnerability where multiple incompatible RPC listeners can be initiated, causing disruptions in the AD DC service. When Samba's RPC server experiences a high load or unresponsiveness, servers intended for non-AD DC purposes (for example, NT4-emulation "classic DCs") can erroneously start and compete for the same unix domain sockets. This issue leads to partial query responses from the AD DC, causing issues such as "The procedure number is out of range" when using tools like Active Directory Users. This flaw allows an attacker to disrupt AD DC services.

CVSS: N/A

1.179 CVE-2023-4091

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A vulnerability was discovered in Samba, where the flaw allows SMB clients to truncate files, even with read-only permissions when the Samba VFS module "acl_xattr" is configured with "acl_xattr:ignore system acls = yes". The SMB protocol allows opening files when the client requests read-only access but then implicitly truncates the opened file to 0 bytes if the client specifies a separate OVERWRITE create disposition request. The issue arises in configurations that bypass kernel file system permissions checks, relying solely on Samba's permissions.

CVSS: N/A

1.180 CVE-2023-3961

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A path traversal vulnerability was identified in Samba when processing client pipe names connecting to Unix domain sockets within a private directory. Samba typically uses this mechanism to connect SMB clients to remote procedure call (RPC) services like SAMR LSA or SPOOLSS, which Samba initiates on demand. However, due to inadequate sanitization of incoming client pipe names, allowing a client to send a pipe name containing Unix directory traversal characters (../). This could result in SMB clients connecting as root to Unix domain sockets outside the private directory. If an attacker or client managed to send a pipe name resolving to an external service using an existing Unix domain socket, it could potentially lead to unauthorized access to the service and consequential adverse events, including compromise or service crashes.

CVSS: N/A

1.181 CVE-2023-42669

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A vulnerability was found in Samba's "rpcecho" development server, a non-Windows RPC server used to test Samba's DCE/RPC stack elements. This vulnerability stems from an RPC function that can be blocked indefinitely. The issue arises because the "rpcecho" service operates with only one worker in the main RPC task, allowing calls to the "rpcecho" server to be blocked for a specified time, causing service disruptions. This disruption is triggered by a "sleep()" call in the "dcesrv_echo_TestSleep()" function under specific conditions. Authenticated users or attackers can exploit this vulnerability to make calls to the "rpcecho" server, requesting it to block for a specified duration, effectively disrupting most services and leading to a complete denial of service on the AD DC. The DoS affects all other services as "rpcecho" runs in the main RPC task.

CVSS: N/A

1.182 CVE-2023-4154

!–> CVE for cpe:2.3:a:samba:samba:4.3.11:::::::*

Summary: A design flaw was found in Samba's DirSync control implementation, which exposes passwords and secrets in Active Directory to privileged users and Read-Only Domain Controllers (RODCs). This flaw allows RODCs and users possessing the GET_CHANGES right to access all attributes, including sensitive secrets and passwords. Even in a default setup, RODC DC accounts, which should only replicate some passwords, can gain access to all domain secrets, including the vital krbtgt, effectively eliminating the RODC / DC distinction. Furthermore, the vulnerability fails to account for error conditions (fail open), like out-of-memory situations, potentially granting access to secret attributes, even under low-privileged attacker influence.

CVSS: N/A

1.183 CVE-2015-1158

!–> CVE for cpe:2.3:a:cups:cups:1.7:-::::::

Summary: The add_job function in scheduler/ipp.c in cupsd in CUPS before 2.0.3 performs incorrect free operations for multiple-value job-originating-host-name attributes, which allows remote attackers to trigger data corruption for reference-counted strings via a crafted (1) IPP_CREATE_JOB or (2) IPP_PRINT_JOB request, as demonstrated by replacing the configuration file and consequently executing arbitrary code.

CVSS: 10.0

1.184 CVE-2015-1159

!–> CVE for cpe:2.3:a:cups:cups:1.7:-::::::

Summary: Cross-site scripting (XSS) vulnerability in the cgi_puts function in cgi-bin/template.c in the template engine in CUPS before 2.0.3 allows remote attackers to inject arbitrary web script or HTML via the QUERY parameter to help/.

CVSS: 4.3

1.185 CVE-2022-4603

!–> CVE for cpe:2.3:a:samba:ppp:2.3.11::::linux::

Summary: A vulnerability classified as problematic has been found in ppp. Affected is the function dumpppp of the file pppdump/pppdump.c of the component pppdump. The manipulation of the argument spkt.buf/rpkt.buf leads to improper validation of array index. The real existence of this vulnerability is still doubted at the moment. The name of the patch is a75fb7b198eed50d769c80c36629f38346882cbf. It is recommended to apply a patch to fix this issue. VDB-216198 is the identifier assigned to this vulnerability. NOTE: pppdump is not used in normal process of setting up a PPP connection, is not installed setuid-root, and is not invoked automatically in any scenario.

CVSS: N/A

1.186 CVE-2020-14760

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 7.5

1.187 CVE-2013-2395

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-1567.

CVSS: 6.8

1.188 CVE-2013-5860

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via vectors related to GIS.

CVSS: 6.8

1.189 CVE-2013-5882

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Stored Procedures.

CVSS: 6.8

1.190 CVE-2016-0504

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0503.

CVSS: 6.8

1.191 CVE-2016-3518

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.

CVSS: 6.8

1.192 CVE-2020-14814

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.193 CVE-2020-14830

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.194 CVE-2020-14837

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.195 CVE-2020-14839

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.196 CVE-2020-14845

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.197 CVE-2020-14846

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.198 CVE-2020-14852

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 6.8

1.199 CVE-2014-2444

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to InnoDB.

CVSS: 6.5

1.200 CVE-2014-2484

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to SRFTS.

CVSS: 6.5

1.201 CVE-2015-2617

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Partition.

CVSS: 6.5

1.202 CVE-2013-3798

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect integrity and availability via unknown vectors related to MemCached.

CVSS: 5.8

1.203 CVE-2017-3454

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).

CVSS: 5.5

1.204 CVE-2017-3455

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).

CVSS: 5.5

1.205 CVE-2019-2731

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.23 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.4 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:L).

CVSS: 5.5

1.206 CVE-2013-1570

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote attackers to affect availability via unknown vectors related to MemCached.

CVSS: 5.0

1.207 CVE-2020-1967

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the “signature_algorithms_cert” TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affect OpenSSL versions prior to 1.1.1d. Fixed in OpenSSL 1.1.1g (Affected 1.1.1d-1.1.1f).

CVSS: 5.0

1.208 CVE-2016-3588

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect integrity and availability via vectors related to Server: InnoDB.

CVSS: 4.9

1.209 CVE-2021-2356

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.34 and prior and 8.0.25 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:H).

CVSS: 4.9

1.210 CVE-2014-0433

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote attackers to affect availability via unknown vectors related to Thread Pooling.

CVSS: 4.3

1.211 CVE-2016-0594

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.21 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.3

1.212 CVE-2015-3152

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Oracle MySQL before 5.7.3, Oracle MySQL Connector/C (aka libmysqlclient) before 6.1.3, and MariaDB before 5.5.44 use the –ssl option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, aka a “BACKRONYM” attack.

CVSS: 4.3

1.213 CVE-2017-3467

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.7.17 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/

CVSS: 4.3

1.214 CVE-2017-3650

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: C API). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/

CVSS: 4.3

1.215 CVE-2018-0735

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a (Affected 1.1.1).

CVSS: 4.3

1.216 CVE-2020-1971

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).

CVSS: 4.3

1.217 CVE-2013-3795

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.

CVSS: 4.0

1.218 CVE-2013-3796

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.

CVSS: 4.0

1.219 CVE-2013-3806

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3811.

CVSS: 4.0

1.220 CVE-2013-3807

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Server Privileges.

CVSS: 4.0

1.221 CVE-2013-5767

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.222 CVE-2013-5786

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-5793.

CVSS: 4.0

1.223 CVE-2013-5894

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 4.0

1.224 CVE-2013-5881

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2014-0431.

CVSS: 4.0

1.225 CVE-2014-2434

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.0

1.226 CVE-2014-2435

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.16 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 4.0

1.227 CVE-2014-2442

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to MyISAM.

CVSS: 4.0

1.228 CVE-2014-2450

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.229 CVE-2014-4233

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SRREP.

CVSS: 4.0

1.230 CVE-2014-4238

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SROPTZR.

CVSS: 4.0

1.231 CVE-2015-0409

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.232 CVE-2015-0405

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to XA.

CVSS: 4.0

1.233 CVE-2015-0423

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.234 CVE-2015-0438

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.235 CVE-2015-0439

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB, a different vulnerability than CVE-2015-4756.

CVSS: 4.0

1.236 CVE-2015-0500

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors.

CVSS: 4.0

1.237 CVE-2015-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.238 CVE-2015-0508

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB, a different vulnerability than CVE-2015-0506.

CVSS: 4.0

1.239 CVE-2015-4756

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB, a different vulnerability than CVE-2015-0439.

CVSS: 4.0

1.240 CVE-2015-4772

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.241 CVE-2015-4730

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.20 and earlier allows remote authenticated users to affect availability via unknown vectors related to Types.

CVSS: 4.0

1.242 CVE-2015-4800

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.

CVSS: 4.0

1.243 CVE-2015-4833

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.

CVSS: 4.0

1.244 CVE-2015-4862

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.0

1.245 CVE-2015-4904

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to libmysqld.

CVSS: 4.0

1.246 CVE-2015-4905

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via vectors related to Server : DML.

CVSS: 4.0

1.247 CVE-2016-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0504.

CVSS: 4.0

1.248 CVE-2016-0595

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 4.0

1.249 CVE-2016-0611

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.250 CVE-2016-3424

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.

CVSS: 4.0

1.251 CVE-2016-3440

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.

CVSS: 4.0

1.252 CVE-2016-5436

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.

CVSS: 4.0

1.253 CVE-2016-5437

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Log.
CVSS: 4.0

1.254 CVE-2016-5441

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Replication.
CVSS: 4.0

1.255 CVE-2016-5442

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Encryption.
CVSS: 4.0

1.256 CVE-2016-5628

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: DML.
CVSS: 4.0

1.257 CVE-2016-5631

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Memcached.
CVSS: 4.0

1.258 CVE-2016-5632

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.
CVSS: 4.0

1.259 CVE-2016-5633

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-8290.

CVSS: 4.0

1.260 CVE-2016-5634

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to RBR.

CVSS: 4.0

1.261 CVE-2016-5635

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Audit.

CVSS: 4.0

1.262 CVE-2017-3251

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.9 (Availability impacts).

CVSS: 4.0

1.263 CVE-2017-3256

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).

CVSS: 4.0

1.264 CVE-2017-3452

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.35 and earlier.

Easily “exploitable” vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.265 CVE-2017-3457

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily “exploitable” vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.266 CVE-2017-3458

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily “exploitable” vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.267 CVE-2017-3459

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.17 and earlier. Easily “exploitable” vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.268 CVE-2017-3460

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.17 and earlier. Easily “exploitable” vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.269 CVE-2017-3465

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily “exploitable” vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 4.0

1.270 CVE-2017-3638

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.271 CVE-2017-3639

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.272 CVE-2017-3640

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier.

Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.273 CVE-2017-3642

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.274 CVE-2017-3643

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.275 CVE-2017-3644

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.276 CVE-2017-3645

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier.

Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.277 CVE-2017-3646

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: X Plugin). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.278 CVE-2017-10165

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.279 CVE-2017-10167

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.280 CVE-2017-10284

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Stored Procedure). Supported versions that are affected are 5.7.18

and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.281 CVE-2017-10296

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.282 CVE-2017-10311

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.283 CVE-2017-10313

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.19 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.284 CVE-2018-3061

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior.

Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.285 CVE-2018-3071

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Audit Log). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.286 CVE-2019-2755

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.287 CVE-2019-2757

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.288 CVE-2022-21417

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior.

Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 4.0

1.289 CVE-2014-4240

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows local users to affect confidentiality and integrity via vectors related to SRREP.

CVSS: 3.6

1.290 CVE-2013-1566

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 3.5

1.291 CVE-2013-1567

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language, a different vulnerability than CVE-2013-2395.

CVSS: 3.5

1.292 CVE-2013-2381

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.10 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server Privileges.

CVSS: 3.5

1.293 CVE-2013-3810

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to XA Transactions.

CVSS: 3.5

1.294 CVE-2013-3811

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-3806.

CVSS: 3.5

1.295 CVE-2013-5793

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-5786.

CVSS: 3.5

1.296 CVE-2014-0427

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via vectors related to FTS.

CVSS: 3.5

1.297 CVE-2014-0431

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2013-5881.

CVSS: 3.5

1.298 CVE-2014-2451

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Privileges.

CVSS: 3.5

1.299 CVE-2015-0385

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.21 and earlier allows remote authenticated users to affect availability via unknown vectors related to Pluggable Auth.

CVSS: 3.5

1.300 CVE-2015-0506

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB, a different vulnerability than CVE-2015-0508.

CVSS: 3.5

1.301 CVE-2015-0507

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.

CVSS: 3.5

1.302 CVE-2015-2567

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.

CVSS: 3.5

1.303 CVE-2015-2639

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Firewall.

CVSS: 3.5

1.304 CVE-2015-2641

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.

CVSS: 3.5

1.305 CVE-2015-4761

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.

CVSS: 3.5

1.306 CVE-2015-4769

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Firewall, a different vulnerability than CVE-2015-4767.

CVSS: 3.5

1.307 CVE-2015-4771

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via vectors related to RBR.

CVSS: 3.5

1.308 CVE-2015-4791

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.

CVSS: 3.5

1.309 CVE-2015-4890

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Replication.

CVSS: 3.5

1.310 CVE-2016-0610

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and MariaDB before 10.0.22 and 10.1.x before 10.1.9 allows remote authenticated users to affect availability via unknown vectors related to InnoDB.

CVSS: 3.5

1.311 CVE-2016-0652

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to DML.

CVSS: 3.5

1.312 CVE-2016-0653

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to FTS.

CVSS: 3.5

1.313 CVE-2016-0654

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0656.

CVSS: 3.5

1.314 CVE-2016-0656

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to InnoDB, a different vulnerability than CVE-2016-0654.

CVSS: 3.5

1.315 CVE-2016-0657

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect confidentiality via vectors related to JSON.

CVSS: 3.5

1.316 CVE-2016-0658

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Optimizer.

CVSS: 3.5

1.317 CVE-2016-0659

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Optimizer.

CVSS: 3.5

1.318 CVE-2016-0662

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Partition.

CVSS: 3.5

1.319 CVE-2016-0663

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.10 and earlier allows local users to affect availability via vectors related to Performance Schema.

CVSS: 3.5

1.320 CVE-2016-8286

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.14 and earlier allows remote authenticated users to affect confidentiality via vectors related to Server: Security: Privileges.

CVSS: 3.5

1.321 CVE-2016-8287

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Replication.

CVSS: 3.5

1.322 CVE-2016-8290

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows remote administrators to affect availability via vectors related to Server: Performance Schema, a different vulnerability than CVE-2016-5633.

CVSS: 3.5

1.323 CVE-2017-3319

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: X Plugin). Supported versions that are affected are 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 3.1 (Confidentiality impacts).

CVSS: 3.5

1.324 CVE-2017-3320

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are

5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 2.4 (Confidentiality impacts).

CVSS: 3.5

1.325 CVE-2017-3468

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.7.17 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).

CVSS: 3.5

1.326 CVE-2017-3529

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: UDF). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.327 CVE-2017-3637

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: X Plugin). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.328 CVE-2019-2741

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Log). Supported versions that are affected are 5.7.26 and prior and 8.0.16 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVSS: 3.5

1.329 CVE-2014-4214

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.17 and earlier allows remote authenticated users to affect availability via vectors related to SRSP.

CVSS: 3.3

1.330 CVE-2016-8289

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.13 and earlier allows local users to affect integrity and availability via vectors related to Server: InnoDB.

CVSS: 3.3

1.331 CVE-2014-0430

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Performance Schema.

CVSS: 2.8

1.332 CVE-2015-0511

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : SP.

CVSS: 2.8

1.333 CVE-2015-2566

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.22 and earlier allows remote authenticated users to affect availability via vectors related to DML.

CVSS: 2.8

1.334 CVE-2016-0607

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to replication.

CVSS: 2.8

1.335 CVE-2016-0667

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Locking.

CVSS: 2.8

1.336 CVE-2019-7317

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.

CVSS: 2.6

1.337 CVE-2013-5770

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Locking.

CVSS: 2.1

1.338 CVE-2015-2661

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows local users to affect availability via unknown vectors related to Client.

CVSS: 2.1

1.339 CVE-2015-4910

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.

CVSS: 2.1

1.340 CVE-2020-15358

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.

CVSS: 2.1

1.341 CVE-2021-22570

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Nullptr dereference when a null char is present in a proto symbol. The symbol is parsed incorrectly, leading to an unchecked call into the proto file's name during generation of the resulting error message. Since the symbol is incorrectly parsed, the file is nullptr. We recommend upgrading to version 3.15.0 or greater.

CVSS: 2.1

1.342 CVE-2022-21444

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.7.37 and prior and 8.0.28 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: 2.1

1.343 CVE-2015-4766

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows local users to affect availability via unknown vectors related to Server : Security : Firewall.

CVSS: 1.9

1.344 CVE-2015-0498

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Replication.

CVSS: 1.7

1.345 CVE-2015-4767

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL Server 5.6.24 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Firewall, a different vulnerability than CVE-2015-4769.

CVSS: 1.7

1.346 CVE-2016-5443

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows local users to affect availability via vectors related to Server: Connection.

CVSS: 1.2

1.347 CVE-2023-21977

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.348 CVE-2023-21980

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).

CVSS: N/A

1.349 CVE-2023-22007

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:*:*:*:*:*:*:*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.7.41 and prior and 8.0.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.350 CVE-2023-22015

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.351 CVE-2023-22026

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.42 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.352 CVE-2023-22028

!–> CVE for cpe:2.3:a:oracle:mysql:5.5.62:::::::*

Summary: Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.43 and prior and 8.0.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVSS: N/A

1.353 CVE-2021-28165

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:::::::

Summary: In Eclipse Jetty 7.2.2 to 9.4.38, 10.0.0.alpha0 to 10.0.1, and 11.0.0.alpha0 to 11.0.1, CPU usage can reach 100% upon receiving a large invalid TLS frame.

CVSS: 7.8

1.354 CVE-2017-7657

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:::::::

Summary: In Eclipse Jetty, versions 9.2.x and older, 9.3.x (all configurations), and 9.4.x (non-default configuration with RFC2616 compliance enabled), transfer-encoding chunks are handled poorly. The chunk length parsing was vulnerable to an integer overflow. Thus a large chunk size could be interpreted as a smaller chunk size and content sent as chunk body could be interpreted as a pipelined request. If Jetty was deployed behind an intermediary that imposed some authorization and that intermediary allowed arbitrarily large chunks to be passed on unchanged, then this flaw could be used to bypass the authorization imposed by the intermediary as the fake pipelined request would not be interpreted by the intermediary as a request.

CVSS: 7.5

1.355 CVE-2017-7658

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: In Eclipse Jetty Server, versions 9.2.x and older, 9.3.x (all non HTTP/1.x configurations), and 9.4.x (all HTTP/1.x configurations), when presented with two content-lengths headers, Jetty ignored the second. When presented with a content-length and a chunked encoding header, the content-length was ignored (as per RFC 2616). If an intermediary decided on the shorter length, but still passed on the longer body, then body content could be interpreted by Jetty as a pipelined request. If the intermediary was imposing authorization, the fake pipelined request would bypass that authorization.

CVSS: 7.5

1.356 CVE-2017-9735

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: Jetty through 9.4.x is prone to a timing channel in util/security/Password.java, which makes it easier for remote attackers to obtain access by observing elapsed times before rejection of incorrect passwords.

CVSS: 5.0

1.357 CVE-2017-7656

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: In Eclipse Jetty, versions 9.2.x and older, 9.3.x (all configurations), and 9.4.x (non-default configuration with RFC2616 compliance enabled), HTTP/0.9 is handled poorly. An HTTP/1 style request line (i.e. method space URI space version) that declares a version of HTTP/0.9 was accepted and treated as a 0.9 request. If deployed behind an intermediary that also accepted and passed through the 0.9 version (but did not act on it), then the response sent could be interpreted by the intermediary as HTTP/1 headers. This could be used to poison the cache if the server allowed the origin client to generate arbitrary content in the response.

CVSS: 5.0

1.358 CVE-2019-10247

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: In Eclipse Jetty version 7.x, 8.x, 9.2.27 and older, 9.3.26 and older, and 9.4.16 and older, the server running on any OS and Jetty version combination will reveal the configured fully qualified directory base resource location on the output of the 404 error for not finding a Context that matches the requested path. The default server behavior on jetty-distribution and jetty-home will include at the end of the Handler tree a DefaultHandler, which is responsible for reporting this 404 error, it presents the various configured contexts as HTML for users to click through to. This produced HTML includes output that contains the configured fully qualified directory base resource location for each context.

CVSS: 5.0

1.359 CVE-2021-28169

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, it is possible for requests to the ConcatServlet with a doubly encoded path to access protected resources within the WEB-INF directory. For example a request to `/concat?/%2557EB-INF/web.xml` can retrieve the web.xml file. This can reveal sensitive information regarding the implementation of a web application.

CVSS: 5.0

1.360 CVE-2022-2048

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: In Eclipse Jetty HTTP/2 server implementation, when encountering an invalid HTTP/2 request, the error handling has a bug that can wind up not properly cleaning up the active connections and associated resources. This can lead to a Denial of Service scenario where there are no enough resources left to process good requests.

CVSS: 5.0

1.361 CVE-2020-27216

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: In Eclipse Jetty versions 1.0 thru 9.4.32.v20200930, 10.0.0.alpha1 thru 10.0.0.beta2, and 11.0.0.alpha1 thru 11.0.0.beta2O, on Unix like systems, the system's temporary directory is shared between all users on that system. A collocated user can observe the process of creating a temporary sub directory in the shared temporary directory and race to complete the creation of the temporary subdirectory. If the attacker wins the race then they will have read and write permission to the subdirectory used to unpack web applications, including their WEB-INF/lib jar files and JSP files. If any code is ever executed out of this temporary directory, this can lead to a local privilege escalation vulnerability.

CVSS: 4.4

1.362 CVE-2022-2047

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: In Eclipse Jetty versions 9.4.0 thru 9.4.46, and 10.0.0 thru 10.0.9, and 11.0.0 thru 11.0.9 versions, the parsing of the authority segment of an http scheme URI, the Jetty HttpURI class improperly detects an invalid input as a hostname. This can lead to failures in a Proxy scenario.

CVSS: 4.0

1.363 CVE-2021-34428

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, if an exception is thrown from the SessionListener#sessionDestroyed() method, then the session ID is not invalidated in the session ID manager. On deployments with clustered sessions and multiple contexts this can result in a session not being invalidated. This can result in an application used on a shared computer being left logged in.

CVSS: 3.6

1.364 CVE-2023-26048

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: Jetty is a java based web server and servlet engine. In affected versions servlets with multipart support (e.g. annotated with `@MultipartConfig`) that call `HttpServletRequest.getParameter()` or `HttpServletRequest.getParts()` may cause `OutOfMemoryError` when the client sends a multipart request with a part that has a name but no filename and very large content. This happens even with the default settings of `fileSizeThreshold=0` which should stream the whole part content to disk. An attacker client may send a large multipart request and cause the server to throw `OutOfMemoryError`. However, the server may be able to recover after the `OutOfMemoryError` and continue its service – although it may take some time. This issue has been patched in versions 9.4.51, 10.0.14, and 11.0.14. Users are advised to upgrade. Users unable to upgrade may set the multipart parameter `maxRequestSize` which must be set to a non-negative value, so the whole multipart content is limited (although still read into memory).

CVSS: N/A

1.365 CVE-2023-26049

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: Jetty is a java based web server and servlet engine. Nonstandard cookie parsing in Jetty may allow an attacker to smuggle cookies within other cookies, or otherwise perform unintended behavior by tampering with the cookie parsing mechanism. If Jetty sees a cookie VALUE that starts with `"` (double quote), it will continue to read the cookie string until it sees a closing quote – even if a semicolon is encountered. So, a cookie header such as: `DISPLAY_LANGUAGE="b; JSESSIONID=1337; c=d"` will be parsed as one cookie, with the name DISPLAY_LANGUAGE and a value of b; JSESSIONID=1337; c=d instead of 3 separate cookies. This has security implications because if, say, JSESSIONID is an HttpOnly cookie, and the DISPLAY_LANGUAGE cookie value is rendered on the page, an attacker can smuggle the JSESSIONID cookie into the DISPLAY_LANGUAGE cookie and thereby exfiltrate it. This is significant when an intermediary is enacting some policy based on cookies, so a smuggled cookie can bypass that policy yet still be seen by the Jetty server or its logging system. This issue has been addressed in versions 9.4.51, 10.0.14, 11.0.14, and 12.0.0.beta0 and users are advised to upgrade. There are no known workarounds for this issue.

CVSS: N/A

1.366 CVE-2023-44487

!–> CVE for cpe:2.3:a:eclipse:jetty:8.1.7:20120910:*:*:*:*:*:*

Summary: The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

CVSS: N/A