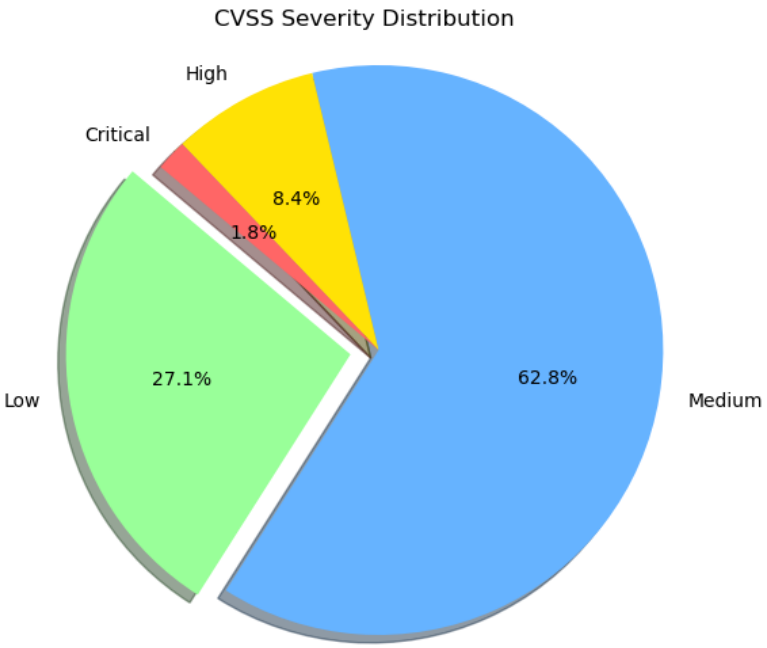
Vulnerability Discovery Results

Monday 8th July, 2024

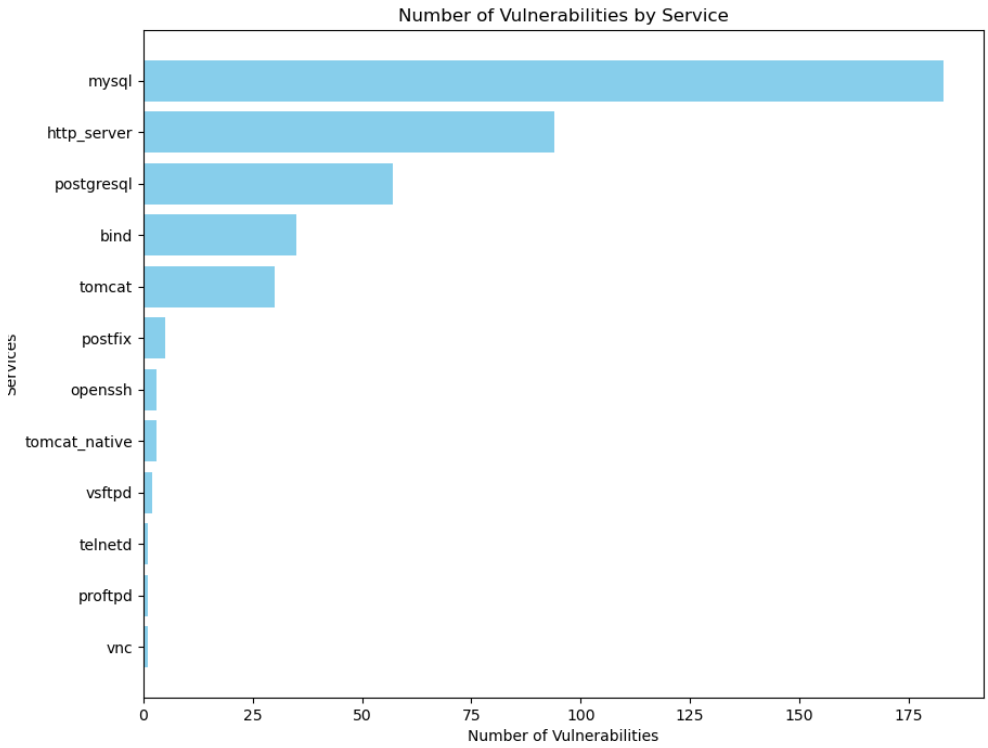
10:23

(UTC+2, PARIS)

CVE	Critical Severity
CVE-2011-2523	10.0
CVE-2008-0122	10.0
CVE-2003-0789	10.0
CVE-2005-2700	10.0
CVE-2010-0425	10.0
CVE-2013-1902	10.0
CVE-2013-1903	10.0
CVE-2016-7048	9.3



(a) Figure 1: Pie Chart



(b) Figure 2: Bar Chart

Details

1.1 CVE-2011-2523

!–> CVE for cpe:2.3:a:vsftpd_project:vsftpd:2.3.4:::::*

Summary: vsftpd 2.3.4 downloaded between 20110630 and 20110703 contains a backdoor which opens a shell on port 6200/tcp.

CVSS: 10.0

1.2 CVE-2021-3618

!–> CVE for cpe:2.3:a:vsftpd_project:vsftpd:2.3.4:::::*

Summary: ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomain to another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

CVSS: 5.8

1.3 CVE-2010-4478

!–> CVE for cpe:2.3:a:openbsd:openssh:4.7p1:::::*

Summary: OpenSSH 5.6 and earlier, when J-PAKE is enabled, does not properly validate the public parameters in the J-PAKE protocol, which allows remote attackers to bypass the need for knowledge of the shared secret, and successfully authenticate, by sending crafted values in each round of the protocol, a related issue to CVE-2010-4252.

CVSS: 7.5

1.4 CVE-2010-4755

!–> CVE for cpe:2.3:a:openbsd:openssh:4.7p1:::::*

Summary: The (1) remote_glob function in sftp-glob.c and the (2) process_put function in sftp.c in OpenSSH 5.8 and earlier, as used in FreeBSD 7.3 and 8.1, NetBSD 5.0.2, OpenBSD 4.7, and other products, allow remote authenticated users to cause a denial of service (CPU and memory consumption) via crafted glob expressions that do not match any pathnames, as demonstrated by glob expressions in SSH_FXP_STAT requests to an sftp daemon, a different vulnerability than CVE-2010-2632.

CVSS: 4.0

1.5 CVE-2008-5161

!–> CVE for cpe:2.3:a:openbsd:openssh:4.7p1:::::*

Summary: Error handling in the SSH protocol in (1) SSH Tectia Client and Server and Connector 4.0 through 4.4.11, 5.0 through 5.2.4, and 5.3 through 5.3.8; Client and Server and ConnectSecure 6.0 through 6.0.4; Server for Linux on IBM System z 6.0.4; Server for IBM z/OS 5.5.1 and earlier, 6.0.0, and 6.0.1; and Client 4.0-J through 4.3.3-J

and 4.0-K through 4.3.10-K; and (2) OpenSSH 4.7p1 and possibly other versions, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors.

CVSS: 2.6

1.6 CVE-2004-0998

!–> CVE for cpe:2.3:a:telnetd:telnetd:0.17.25:::::*

Summary: Format string vulnerability in telnetd-ssl 0.17 and earlier allows remote attackers to execute arbitrary code.

CVSS: 7.5

1.7 CVE-2011-0411

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: The STARTTLS implementation in Postfix 2.4.x before 2.4.16, 2.5.x before 2.5.12, 2.6.x before 2.6.9, and 2.7.x before 2.7.3 does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack.

CVSS: 6.8

1.8 CVE-2011-1720

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: The SMTP server in Postfix before 2.5.13, 2.6.x before 2.6.10, 2.7.x before 2.7.4, and 2.8.x before 2.8.3, when certain Cyrus SASL authentication methods are enabled, does not create a new server handle after client authentication fails, which allows remote attackers to cause a denial of service (heap memory corruption and daemon crash) or possibly execute arbitrary code via an invalid AUTH command with one method followed by an AUTH command with a different method.

CVSS: 6.8

1.9 CVE-2017-10140

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain privileges by leveraging undocumented functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.

CVSS: 4.6

1.10 CVE-2008-3889

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: Postfix 2.4 before 2.4.9, 2.5 before 2.5.5, and 2.6 before 2.6-20080902, when used with the Linux 2.6 kernel, leaks epoll file descriptors during execution of "non-Postfix" commands, which allows local users to cause a denial of service (application

slowdown or exit) via a crafted command, as demonstrated by a command in a .forward file.

CVSS: 2.1

1.11 CVE-2023-51764

!–> CVE for cpe:2.3:a:postfix:postfix:2.4:::::*

Summary: Postfix through 3.8.5 allows SMTP smuggling unless configured with smtpd_data_restrictions=reject_unauth_pipelining and smtpd_discard_ehlo_keywords=chunking (or certain other options that exist in recent versions). Remote attackers can use a published exploitation technique to inject e-mail messages with a spoofed MAIL FROM address, allowing bypass of an SPF protection mechanism. This occurs because Postfix supports . but some other popular e-mail servers do not. To prevent attack variants (by always disallowing without), a different solution is required, such as the smtpd_forbid_bare_newline=yes option with a Postfix minimum version of 3.5.23, 3.6.13, 3.7.9, 3.8.4, or 3.9.

CVSS: N/A

1.12 CVE-2008-0122

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: Off-by-one error in the inet_network function in libbind in ISC BIND 9.4.2 and earlier, as used in libc in FreeBSD 6.2 through 7.0-PRERELEASE, allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted input that triggers memory corruption.

CVSS: 10.0

1.13 CVE-2012-1667

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.x before 9.7.6-P1, 9.8.x before 9.8.3-P1, 9.9.x before 9.9.1-P1, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P1 does not properly handle resource records with a zero-length RDATA section, which allows remote DNS servers to cause a denial of service (daemon crash or data corruption) or obtain sensitive information from process memory via a crafted record.

CVSS: 8.5

1.14 CVE-2012-4244

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.x before 9.7.6-P3, 9.8.x before 9.8.3-P3, 9.9.x before 9.9.1-P3, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P3 allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for a long resource record.

CVSS: 7.8

1.15 CVE-2012-5166

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.x before 9.7.6-P4, 9.8.x before 9.8.3-P4, 9.9.x before 9.9.1-P4, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P4 allows remote attackers to cause a denial of service (named daemon hang) via unspecified combinations of resource records.

CVSS: 7.8

1.16 CVE-2014-8500

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allows remote attackers to cause a denial of service (memory consumption and named crash) via a large or infinite number of referrals.

CVSS: 7.8

1.17 CVE-2015-5477

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.

CVSS: 7.8

1.18 CVE-2015-5722

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.

CVSS: 7.8

1.19 CVE-2016-2776

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.

CVSS: 7.8

1.20 CVE-2010-0382

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta handles out-of-bailiwick data accompanying a secure response without re-fetching from the original source, which allows remote attackers to have

an unspecified impact via a crafted response, aka Bug 20819. NOTE: this vulnerability exists because of a regression during the fix for CVE-2009-4022.

CVSS: 7.6

1.21 CVE-2015-8461

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: Race condition in resolver.c in named in ISC BIND 9.9.8 before 9.9.8-P2 and 9.10.3 before 9.10.3-P2 allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via unspecified vectors.

CVSS: 7.1

1.22 CVE-2015-5986

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: openpgpkey_61.c in named in ISC BIND 9.9.7 before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a crafted DNS response.

CVSS: 7.1

1.23 CVE-2009-0025

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: BIND 9.6.0, 9.5.1, 9.5.0, 9.4.3, and earlier does not properly check the return value from the OpenSSL DSA_verify function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077.

CVSS: 6.8

1.24 CVE-2015-8704

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: apl_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record.

CVSS: 6.8

1.25 CVE-2015-8705

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: buffer.c in named in ISC BIND 9.10.x before 9.10.3-P3, when debug logging is enabled, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit, or daemon crash) or possibly have unspecified other impact via (1) OPT data or (2) an ECS option.

CVSS: 6.6

1.26 CVE-2010-3614

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: named in ISC BIND 9.x before 9.6.2-P3, 9.7.x before 9.7.2-P3, 9.4-ESV before 9.4-ESV-R4, and 9.6-ESV before 9.6-ESV-R3 does not properly determine the security status of an NS RRset during a DNSKEY algorithm rollover, which might allow remote attackers to cause a denial of service (DNSSEC validation error) by triggering a rollover.

CVSS: 6.4

1.27 CVE-2002-0400

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9 before 9.2.1 allows remote attackers to cause a denial of service (shutdown) via a malformed DNS packet that triggers an error condition that is not properly handled when the rdataset parameter to the dns_message_findtype() function in message.c is not NULL, aka DoS_findtype.

CVSS: 5.0

1.28 CVE-2006-2073

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: Unspecified vulnerability in ISC BIND allows remote attackers to cause a denial of service via a crafted DNS message with a “broken” TSIG, as demonstrated by the OUSPG PROTOS DNS test suite.

CVSS: 5.0

1.29 CVE-2011-1910

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: Off-by-one error in named in ISC BIND 9.x before 9.7.3-P1, 9.8.x before 9.8.0-P2, 9.4-ESV before 9.4-ESV-R4-P1, and 9.6-ESV before 9.6-ESV-R4-P1 allows remote DNS servers to cause a denial of service (assertion failure and daemon exit) via a negative response containing large RRSIG RRsets.

CVSS: 5.0

1.30 CVE-2011-4313

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: query.c in ISC BIND 9.0.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5, 9.6-ESV through 9.6-ESV-R5, 9.7.0 through 9.7.4, 9.8.0 through 9.8.1, and 9.9.0a1 through 9.9.0b1 allows remote attackers to cause a denial of service (assertion failure and named exit) via unknown vectors related to recursive DNS queries, error logging, and the caching of an invalid record by the resolver.

CVSS: 5.0

1.31 CVE-2012-1033

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: The resolver in ISC BIND 9 through 9.8.1-P1 overwrites cached server names and TTL values in NS records during the processing of a response to an A record query, which allows remote attackers to trigger continued resolvability of revoked domain names via a “ghost domain names” attack.

CVSS: 5.0

1.32 CVE-2015-8000

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.

CVSS: 5.0

1.33 CVE-2016-9444

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.

CVSS: 5.0

1.34 CVE-2006-4095

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: BIND before 9.2.6-P1 and 9.3.x before 9.3.2-P1 allows remote attackers to cause a denial of service (crash) via certain SIG queries, which cause an assertion failure when multiple RRsets are returned.

CVSS: 5.0

1.35 CVE-2009-0265

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: Internet Systems Consortium (ISC) BIND 9.6.0 and earlier does not properly check the return value from the OpenSSL EVP_VerifyFinal function, which allows remote attackers to bypass validation of the certificate chain via a malformed SSL/TLS signature, a similar vulnerability to CVE-2008-5077 and CVE-2009-0025.

CVSS: 5.0

1.36 CVE-2016-9131

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.

CVSS: 5.0

1.37 CVE-2001-0497

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: dnskeygen in BIND 8.2.4 and earlier, and dnssec-keygen in BIND 9.1.2 and earlier, set insecure permissions for a HMAC-MD5 shared secret key file used for DNS Transactional Signatures (TSIG), which allows attackers to obtain the keys and perform dynamic DNS updates.

CVSS: 4.6

1.38 CVE-2007-0494

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.0.x, 9.1.x, 9.2.0 up to 9.2.7, 9.3.0 up to 9.3.3, 9.4.0a1 up to 9.4.0a6, 9.4.0b1 up to 9.4.0b4, 9.4.0rc1, and 9.5.0a1 (Bind Forum only) allows remote attackers to cause a denial of service (exit) via a type * (ANY) DNS query response that contains multiple RRsets, which triggers an assertion error, aka the "DNSSEC Validation" vulnerability.

CVSS: 4.3

1.39 CVE-2007-2926

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9 through 9.5.0a5 uses a weak random number generator during generation of DNS query ids when answering resolver questions or sending NOTIFY messages to slave name servers, which makes it easier for remote attackers to guess the next query id and perform DNS cache poisoning.

CVSS: 4.3

1.40 CVE-2010-0097

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta does not properly validate DNSSEC (1) NSEC and (2) NSEC3 records, which allows remote attackers to add the Authenticated Data (AD) flag to a forged NXDOMAIN response for an existing domain.

CVSS: 4.3

1.41 CVE-2010-3762

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND before 9.7.2-P2, when DNSSEC validation is enabled, does not properly handle certain bad signatures if multiple trust anchors exist for a single zone, which allows remote attackers to cause a denial of service (daemon crash) via a DNS query.

CVSS: 4.3

1.42 CVE-2016-2775

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND 9.x before 9.9.9-P2, 9.10.x before 9.10.4-P2, and 9.11.x before 9.11.0b2, when lwresd or the named lwres option is enabled, allows remote attackers to cause a denial of service (daemon crash) via a long request that uses the lightweight resolver protocol.

CVSS: 4.3

1.43 CVE-2010-0290

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: Unspecified vulnerability in ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P5, 9.5 before 9.5.2-P2, 9.6 before 9.6.1-P3, and 9.7.0 beta, with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains (1) CNAME or (2) DNAME records, which do not have the intended validation before caching, aka Bug 20737. NOTE: this vulnerability exists because of an incomplete fix for CVE-2009-4022.

CVSS: 4.0

1.44 CVE-2016-6170

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: ISC BIND through 9.9.9-P1, 9.10.x through 9.10.4-P1, and 9.11.x through 9.11.0b1 allows primary DNS servers to cause a denial of service (secondary DNS server crash) via a large AXFR response, and possibly allows IXFR servers to cause a denial of service (IXFR client crash) via a large IXFR response and allows remote authenticated users to cause a denial of service (primary DNS server crash) via a large UPDATE message.

CVSS: 4.0

1.45 CVE-2018-5741

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: To provide fine-grained controls over the ability to use Dynamic DNS (DDNS) to update records in a zone, BIND 9 provides a feature called update-policy. Various rules can be configured to limit the types of updates that can be performed by a client, depending on the key used when sending the update request. Unfortunately, some rule types were not initially documented, and when documentation for them was added to the Administrator Reference Manual (ARM) in change #3112, the language that was added to the ARM at that time incorrectly described the behavior of two rule types, krb5-subdomain and ms-subdomain. This incorrect documentation could mislead operators into believing that policies they had configured were more restrictive than they actually were. This affects BIND versions prior to BIND 9.11.5 and BIND 9.12.3.

CVSS: 4.0

1.46 CVE-2009-4022

!–> CVE for cpe:2.3:a:isc:bind:9.0:::::*

Summary: Unspecified vulnerability in ISC BIND 9.0.x through 9.3.x, 9.4 before 9.4.3-P4, 9.5 before 9.5.2-P1, 9.6 before 9.6.1-P2, and 9.7 beta before 9.7.0b3, with DNSSEC validation enabled and checking disabled (CD), allows remote attackers to conduct DNS cache poisoning attacks by receiving a recursive client query and sending a response that contains an Additional section with crafted data, which is not properly handled when the response is processed "at the same time as requesting DNSSEC records (DO)," aka Bug 20438.

CVSS: 2.6

1.47 CVE-2003-0789

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: mod_cgid in Apache before 2.0.48, when using a threaded MPM, does not properly handle CGI redirect paths, which could cause Apache to send the output of a CGI program to the wrong client.

CVSS: 10.0

1.48 CVE-2005-2700

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: ssl_engine_kernel.c in mod_ssl before 2.8.24, when using "SSLVerifyClient optional" in the global virtual host configuration, does not properly enforce "SSLVerifyClient require" in a per-location context, which allows remote attackers to bypass intended access restrictions.

CVSS: 10.0

1.49 CVE-2010-0425

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: modules/arch/win32/mod_isapi.c in mod_isapi in the Apache HTTP Server 2.0.37 through 2.0.63, 2.2.0 through 2.2.14, and 2.3.x before 2.3.7, when running on Windows, does not ensure that request processing is complete before calling isapi_unload for an ISAPI .dll module, which allows remote attackers to execute arbitrary code via unspecified vectors related to a crafted request, a reset packet, and "orphaned callback pointers."

CVSS: 10.0

1.50 CVE-2011-3192

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.

CVSS: 7.8

1.51 CVE-2002-0392

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache 1.3 through 1.3.24, and Apache 2.0 through 2.0.36, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a chunk-encoded HTTP request that causes Apache to use an incorrect size.

CVSS: 7.5

1.52 CVE-2002-0661

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Directory traversal vulnerability in Apache 2.0 through 2.0.39 on Windows, OS2, and Netware allows remote attackers to read arbitrary files and execute commands via .. (dot dot) sequences containing (backslash) characters.

CVSS: 7.5

1.53 CVE-2003-0016

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache before 2.0.44, when running on unpatched Windows 9x and Me operating systems, allows remote attackers to cause a denial of service or execute arbitrary code via an HTTP request containing MS-DOS device names.

CVSS: 7.5

1.54 CVE-2004-0488

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Stack-based buffer overflow in the ssl_util_uuencode_binary function in ssl_util.c for Apache mod_ssl, when mod_ssl is configured to trust the issuing CA, may allow remote attackers to execute arbitrary code via a client certificate with a long subject DN.

CVSS: 7.5

1.55 CVE-2004-0885

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_ssl module in Apache 2.0.35 through 2.0.52, when using the "SSLCipherSuite" directive in directory or location context, allows remote clients to bypass intended restrictions by using any cipher suite that is allowed by the virtual host configuration.

CVSS: 7.5

1.56 CVE-2008-2384

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: SQL injection vulnerability in mod_auth_mysql.c in the mod-auth-mysql (aka libapache2-mod-auth-mysql) module for the Apache HTTP Server 2.x, when configured to use a multibyte character set that allows a (backslash) as part of the character

encoding, allows remote attackers to execute arbitrary SQL commands via unspecified inputs in a login request.

CVSS: 7.5

1.57 CVE-2021-39275

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.58 CVE-2021-44790

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.59 CVE-2022-22720

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.60 CVE-2022-31813

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.61 CVE-2003-0542

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: Multiple stack-based buffer overflows in (1) mod_alias and (2) mod_rewrite for Apache before 1.3.29 allow attackers to create configuration files to cause a denial of service (crash) or execute arbitrary code via a regular expression with more than 9 captures.

CVSS: 7.2

1.62 CVE-2004-2343

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache HTTP Server 2.0.47 and earlier allows local users to bypass .htaccess file restrictions, as specified in httpd.conf with directives such as Deny From All, by using an ErrorDocument directive. NOTE: the vendor has disputed this issue, since the .htaccess mechanism is only intended to restrict external web access, and a local user already has the privileges to perform the same operations without using ErrorDocument

CVSS: 7.2

1.63 CVE-2009-1891

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_deflate module in Apache httpd 2.2.11 and earlier compresses large files until completion even after the associated network connection is closed, which allows remote attackers to cause a denial of service (CPU consumption).

CVSS: 7.1

1.64 CVE-2002-0840

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in the default error page of Apache 2.0 before 2.0.43, and 1.3.x up to 1.3.26, when UseCanonicalName is "Off" and support for wildcard DNS is present, allows remote attackers to execute script as other web page visitors via the Host: header, a different vulnerability than CAN-2002-1157.

CVSS: 6.8

1.65 CVE-2006-4154

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Format string vulnerability in the mod_tcl module 1.0 for Apache 2.x allows context-dependent attackers to execute arbitrary code via format string specifiers that are not properly handled in a set_var function call in (1) tcl_cmds.c and (2) tcl_core.c.

CVSS: 6.8

1.66 CVE-2021-40438

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

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

1.67 CVE-2003-0192

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache 2 before 2.0.47, and certain versions of mod_ssl for Apache 1.3, do not properly handle “certain sequences of per-directory renegotiations and the SSL-CipherSuite directive being used to upgrade from a weak ciphersuite to a strong one,” which could cause Apache to use the weak ciphersuite.

CVSS: 6.4

1.68 CVE-2017-9788

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

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

1.69 CVE-2022-28615

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

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

1.70 CVE-2009-3555

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The TLS protocol, and the SSL protocol 3.0 and possibly earlier, as used in Microsoft Internet Information Services (IIS) 7.0, mod_ssl in the Apache HTTP Server 2.2.14 and earlier, OpenSSL before 0.9.8l, GnuTLS 2.8.5 and earlier, Mozilla Network Security Services (NSS) 3.12.4 and earlier, multiple Cisco products, and other products, does not properly associate renegotiation handshakes with an existing connection, which allows man-in-the-middle attackers to insert data into HTTPS sessions, and possibly other types of sessions protected by TLS or SSL, by sending an unauthenticated request that is processed retroactively by a server in a post-renegotiation context, related to a “plaintext injection” attack, aka the “Project Mogul” issue.

CVSS: 5.8

1.71 CVE-2022-22721

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

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

1.72 CVE-2005-3357

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: mod_ssl in Apache 2.0 up to 2.0.55, when configured with an SSL vhost with access control and a custom error 400 error page, allows remote attackers to cause a denial of service (application crash) via a non-SSL request to an SSL port, which triggers a NULL pointer dereference.

CVSS: 5.4

1.73 CVE-2013-1862

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.

CVSS: 5.1

1.74 CVE-2001-1556

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: The log files in Apache web server contain information directly supplied by clients and does not filter or quote control characters, which could allow remote attackers to hide HTTP requests and spoof source IP addresses when logs are viewed with UNIX programs such as cat, tail, and grep.

CVSS: 5.0

1.75 CVE-2002-0654

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: Apache 2.0 through 2.0.39 on Windows, OS2, and Netware allows remote attackers to determine the full pathname of the server via (1) a request for a .var file, which leaks the pathname in the resulting error message, or (2) via an error message that occurs when a script (child process) cannot be invoked.

CVSS: 5.0

1.76 CVE-2002-1593

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: mod_dav in Apache before 2.0.42 does not properly handle versioning hooks, which may allow remote attackers to kill a child process via a null dereference and cause a denial of service (CPU consumption) in a preforked multi-processing module.

CVSS: 5.0

1.77 CVE-2003-0017

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: Apache 2.0 before 2.0.44 on Windows platforms allows remote attackers to obtain certain files via an HTTP request that ends in certain illegal characters such as ">", which causes a different filename to be processed and served.

CVSS: 5.0

1.78 CVE-2003-0020

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: Apache does not filter terminal escape sequences from its error logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences.

CVSS: 5.0

1.79 CVE-2003-0083

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: Apache 1.3 before 1.3.25 and Apache 2.0 before version 2.0.46 does not filter terminal escape sequences from its access logs, which could make it easier for attackers to insert those sequences into terminal emulators containing vulnerabilities related to escape sequences, a different vulnerability than CVE-2003-0020.

CVSS: 5.0

1.80 CVE-2003-0132

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: A memory leak in Apache 2.0 through 2.0.44 allows remote attackers to cause a denial of service (memory consumption) via large chunks of linefeed characters, which causes Apache to allocate 80 bytes for each linefeed.

CVSS: 5.0

1.81 CVE-2003-0134

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: Unknown vulnerability in filestat.c for Apache running on OS2, versions 2.0 through 2.0.45, allows unknown attackers to cause a denial of service via requests related to device names.

CVSS: 5.0

1.82 CVE-2003-0253

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: The prefork MPM in Apache 2 before 2.0.47 does not properly handle certain errors from accept, which could lead to a denial of service.

CVSS: 5.0

1.83 CVE-2003-0254

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache 2 before 2.0.47, when running on an IPv6 host, allows attackers to cause a denial of service (CPU consumption by infinite loop) when the FTP proxy server fails to create an IPv6 socket.

CVSS: 5.0

1.84 CVE-2004-0113

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Memory leak in ssl_engine_io.c for mod_ssl in Apache 2 before 2.0.49 allows remote attackers to cause a denial of service (memory consumption) via plain HTTP requests to the SSL port of an SSL-enabled server.

CVSS: 5.0

1.85 CVE-2004-0174

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache 1.4.x before 1.3.30, and 2.0.x before 2.0.49, when using multiple listening sockets on certain platforms, allows remote attackers to cause a denial of service (blocked new connections) via a "short-lived connection on a rarely-accessed listening socket."

CVSS: 5.0

1.86 CVE-2004-0809

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_dav module in Apache 2.0.50 and earlier allows remote attackers to cause a denial of service (child process crash) via a certain sequence of LOCK requests for a location that allows WebDAV authoring access.

CVSS: 5.0

1.87 CVE-2004-0748

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: mod_ssl in Apache 2.0.50 and earlier allows remote attackers to cause a denial of service (CPU consumption) by aborting an SSL connection in a way that causes an Apache child process to enter an infinite loop.

CVSS: 5.0

1.88 CVE-2004-0786

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The IPv6 URI parsing routines in the apr-util library for Apache 2.0.50 and earlier allow remote attackers to cause a denial of service (child process crash) via a certain URI, as demonstrated using the Codenomicon HTTP Test Tool.

CVSS: 5.0

1.89 CVE-2004-0263

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: PHP 4.3.4 and earlier in Apache 1.x and 2.x (mod_php) can leak global variables between virtual hosts that are handled by the same Apache child process but have different settings, which could allow remote attackers to obtain sensitive information.

CVSS: 5.0

1.90 CVE-2004-0942

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache webserver 2.0.52 and earlier allows remote attackers to cause a denial of service (CPU consumption) via an HTTP GET request with a MIME header containing multiple lines with a large number of space characters.

CVSS: 5.0

1.91 CVE-2005-1268

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Off-by-one error in the mod_ssl Certificate Revocation List (CRL) verification callback in Apache, when configured to use a CRL, allows remote attackers to cause a denial of service (child process crash) via a CRL that causes a buffer overflow of one null byte.

CVSS: 5.0

1.92 CVE-2005-2728

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The byte-range filter in Apache 2.0 before 2.0.54 allows remote attackers to cause a denial of service (memory consumption) via an HTTP header with a large Range field.

CVSS: 5.0

1.93 CVE-2005-2970

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Memory leak in the worker MPM (worker.c) for Apache 2, in certain circumstances, allows remote attackers to cause a denial of service (memory consumption) via aborted connections, which prevents the memory for the transaction pool from being reused for other connections.

CVSS: 5.0

1.94 CVE-2007-3847

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The date handling code in modules/proxy/proxy_util.c (mod_proxy) in Apache 2.3.0, when using a threaded MPM, allows remote origin servers to cause a denial of service (caching forward proxy process crash) via crafted date headers that trigger a buffer over-read.

CVSS: 5.0

1.95 CVE-2008-2364

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.

CVSS: 5.0

1.96 CVE-2009-3095

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_proxy_ftp module in the Apache HTTP Server allows remote attackers to bypass intended access restrictions and send arbitrary commands to an FTP server via vectors related to the embedding of these commands in the Authorization HTTP header, as demonstrated by a certain module in VulnDisco Pack Professional 8.11.

CVSS: 5.0

1.97 CVE-2009-3720

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The updatePosition function in lib/xmltok_impl.c in libexpat in Expat 2.0.1, as used in Python, PyXML, w3c-libwww, and other software, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with crafted UTF-8 sequences that trigger a buffer over-read, a different vulnerability than CVE-2009-2625.

CVSS: 5.0

1.98 CVE-2009-3560

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The big2_toUtf8 function in lib/xmltok.c in libexpat in Expat 2.0.1, as used in the XML-Twig module for Perl, allows context-dependent attackers to cause a denial of service (application crash) via an XML document with malformed UTF-8 sequences that trigger a buffer over-read, related to the doProlog function in lib/xmlparse.c, a different vulnerability than CVE-2009-2625 and CVE-2009-3720.

CVSS: 5.0

1.99 CVE-2010-1452

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The (1) mod_cache and (2) mod_dav modules in the Apache HTTP Server 2.2.x before 2.2.16 allow remote attackers to cause a denial of service (process crash) via a request that lacks a path.

CVSS: 5.0

1.100 CVE-2010-1623

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Memory leak in the apr_brigade_split_line function in buckets/apr_brigade.c in the Apache Portable Runtime Utility library (aka APR-util) before 1.3.10, as used in the mod_reqtimeout module in the Apache HTTP Server and other software, allows remote attackers to cause a denial of service (memory consumption) via unspecified vectors related to the destruction of an APR bucket.

CVSS: 5.0

1.101 CVE-2011-3368

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.

CVSS: 5.0

1.102 CVE-2007-6750

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The Apache HTTP Server 1.x and 2.x allows remote attackers to cause a denial of service (daemon outage) via partial HTTP requests, as demonstrated by Slowloris, related to the lack of the mod_reqtimeout module in versions before 2.2.15.

CVSS: 5.0

1.103 CVE-2015-0228

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

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

1.104 CVE-2017-9798

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

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

1.105 CVE-2018-1303

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.106 CVE-2021-34798

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.107 CVE-2022-22719

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.108 CVE-2022-28330

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.109 CVE-2022-28614

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.110 CVE-2022-29404

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.111 CVE-2022-30556

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

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

1.112 CVE-2007-3304

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Apache httpd 1.3.37, 2.0.59, and 2.2.4 with the Prefork MPM module, allows local users to cause a denial of service by modifying the worker_score and process_score arrays to reference an arbitrary process ID, which is sent a SIGUSR1 signal from the master process, aka "SIGUSR1 killer."

CVSS: 4.7

1.113 CVE-2004-0747

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Buffer overflow in Apache 2.0.50 and earlier allows local users to gain apache privileges via a .htaccess file that causes the overflow during expansion of environment variables.

CVSS: 4.6

1.114 CVE-2012-0031

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.

CVSS: 4.6

1.115 CVE-2011-3607

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.

CVSS: 4.4

1.116 CVE-2003-1307

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_php module for the Apache HTTP Server allows local users with write access to PHP scripts to send signals to the server's process group and use the server's file descriptors, as demonstrated by sending a STOP signal, then intercepting incoming connections on the server's TCP port. NOTE: the PHP developer has disputed this vulnerability, saying "The opened file descriptors are opened by Apache. It is the job of Apache to protect them … Not a bug in PHP.

CVSS: 4.3

1.117 CVE-2005-2088

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The Apache HTTP server before 1.3.34, and 2.0.x before 2.0.55, when acting as an HTTP proxy, allows remote attackers to poison the web cache, bypass web application firewall protection, and conduct XSS attacks via an HTTP request with both a "Transfer-Encoding: chunked" header and a Content-Length header, which causes Apache to incorrectly handle and forward the body of the request in a way that causes the receiving server to process it as a separate HTTP request, aka "HTTP Request Smuggling."

CVSS: 4.3

1.118 CVE-2005-3352

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in the mod_imap module of Apache httpd before 1.3.35-dev and Apache httpd 2.0.x before 2.0.56-dev allows remote attackers to inject arbitrary web script or HTML via the Referer when using image maps.

CVSS: 4.3

1.119 CVE-2006-5752

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in mod_status.c in the mod_status module in Apache HTTP Server (httpd), when ExtendedStatus is enabled and a public server-status page is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors involving charsets with browsers that perform "charset detection" when the content-type is not specified.

CVSS: 4.3

1.120 CVE-2007-4465

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in mod_autoindex.c in the Apache HTTP Server before 2.2.6, when the charset on a server-generated page is not defined, allows remote attackers to inject arbitrary web script or HTML via the P parameter using the UTF-7 charset. NOTE: it could be argued that this issue is due to a design limitation of browsers that attempt to perform automatic content type detection.

CVSS: 4.3

1.121 CVE-2007-5000

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in the (1) mod_imap module in the Apache HTTP Server 1.3.0 through 1.3.39 and 2.0.35 through 2.0.61 and the (2) mod_imagemap module in the Apache HTTP Server 2.2.0 through 2.2.6 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVSS: 4.3

1.122 CVE-2007-6388

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in mod_status in the Apache HTTP Server 2.2.0 through 2.2.6, 2.0.35 through 2.0.61, and 1.3.2 through 1.3.39, when the server-status page is enabled, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVSS: 4.3

1.123 CVE-2008-0005

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: mod_proxy_ftp in Apache 2.2.x before 2.2.7-dev, 2.0.x before 2.0.62-dev, and 1.3.x before 1.3.40-dev does not define a charset, which allows remote attackers to conduct cross-site scripting (XSS) attacks using UTF-7 encoding.

CVSS: 4.3

1.124 CVE-2008-2168

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in Apache 2.2.6 and earlier allows remote attackers to inject arbitrary web script or HTML via UTF-7 encoded URLs that are not properly handled when displaying the 403 Forbidden error page.

CVSS: 4.3

1.125 CVE-2008-2939

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Cross-site scripting (XSS) vulnerability in proxy_ftp.c in the mod_proxy_ftp module in Apache 2.0.63 and earlier, and mod_proxy_ftp.c in the mod_proxy_ftp module in Apache 2.2.9 and earlier 2.2 versions, allows remote attackers to inject arbitrary web script or HTML via a wildcard in the last directory component in the pathname in an FTP URI.

CVSS: 4.3

1.126 CVE-2010-0434

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The ap_read_request function in server/protocol.c in the Apache HTTP Server 2.2.x before 2.2.15, when a multithreaded MPM is used, does not properly handle headers in subrequests in certain circumstances involving a parent request that has a body, which might allow remote attackers to obtain sensitive information via a crafted request that triggers access to memory locations associated with an earlier request.

CVSS: 4.3

1.127 CVE-2011-0419

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: Stack consumption vulnerability in the fnmatch implementation in apr_fnmatch.c in the Apache Portable Runtime (APR) library before 1.4.3 and the Apache HTTP Server before 2.2.18, and in fnmatch.c in libc in NetBSD 5.1, OpenBSD 4.8, FreeBSD, Apple Mac OS X 10.6, Oracle Solaris 10, and Android, allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via *? sequences in the first argument, as demonstrated by attacks against mod_autoindex in httpd.

CVSS: 4.3

1.128 CVE-2011-3639

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

CVSS: 4.3

1.129 CVE-2011-4317

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an @ (at sign) character and a : (colon) character in invalid positions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

CVSS: 4.3

1.130 CVE-2012-0053

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::::*

Summary: protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1) long or (2) malformed header in conjunction with crafted web script.

CVSS: 4.3

1.131 CVE-2018-1301

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.132 CVE-2018-1302

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.133 CVE-2016-8612

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.134 CVE-2009-3094

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: The ap_proxy_ftp_handler function in modules/proxy/proxy_ftp.c in the mod_proxy_ftp module in the Apache HTTP Server 2.0.63 and 2.2.13 allows remote FTP servers to cause a denial of service (NULL pointer dereference and child process crash) via a malformed reply to an EPSV command.

CVSS: 2.6

1.135 CVE-2004-1834

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: mod_disk_cache in Apache 2.0 through 2.0.49 stores client headers, including authentication information, on the hard disk, which could allow local users to gain sensitive information.

CVSS: 2.1

1.136 CVE-2011-4415

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

Summary: The ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, does not restrict the size of values of environment variables, which allows local users to cause a denial of service (memory consumption or NULL pointer dereference) via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, related to (1) the "len +=" statement and (2) the apr_pcalloc function call, a different vulnerability than CVE-2011-3607.

CVSS: 1.2

1.137 CVE-2006-20001

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.138 CVE-2022-37436

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.139 CVE-2023-31122

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.140 CVE-2023-45802

!–> CVE for cpe:2.3:a:apache:http_server:2.0.36:::::*

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

1.141 CVE-2006-6563

!–> CVE for cpe:2.3:a:proftpd_project:proftpd:1.3.0:::::*

Summary: Stack-based buffer overflow in the pr_ctrls_recv_request function in ctrls.c in the mod_ctrls module in ProFTPD before 1.3.1rc1 allows local users to execute arbitrary code via a large reqarglen length value.

CVSS: 6.6

1.142 CVE-2009-2446

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Multiple format string vulnerabilities in the dispatch_command function in libmysqld/sql_parse.cc in mysqld in MySQL 4.0.0 through 5.0.83 allow remote authenticated users to cause a denial of service (daemon crash) and possibly have unspecified other impact via format string specifiers in a database name in a (1) COM_CREATE_DB or (2) COM_DROP_DB request. NOTE: some of these details are obtained from third party information.

CVSS: 8.5

1.143 CVE-2009-4484

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Multiple stack-based buffer overflows in the CertDecoder::GetName function in src/asn.cpp in TaoCrypt in yaSSL before 1.9.9, as used in mysqld in MySQL 5.0.x before 5.0.90, MySQL 5.1.x before 5.1.43, MySQL 5.5.x through 5.5.0-m2, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption and daemon crash) by establishing an SSL connection and sending an X.509 client certificate with a crafted name field, as demonstrated by mysql_overflow1.py and the vd_mysql5 module in VulnDisco Pack Professional 8.11. NOTE: this was originally reported for MySQL 5.0.51a.

CVSS: 7.5

1.144 CVE-2020-14760

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.145 CVE-2013-2395

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.146 CVE-2013-5860

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.147 CVE-2013-5882

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.148 CVE-2016-0504

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.149 CVE-2016-3518

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.150 CVE-2020-14814

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.151 CVE-2020-14830

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.152 CVE-2020-14837

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.153 CVE-2020-14839

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.154 CVE-2020-14845

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.155 CVE-2020-14846

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.156 CVE-2020-14852

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.157 CVE-2012-4414

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Multiple SQL injection vulnerabilities in the replication code in Oracle MySQL possibly before 5.5.29, and MariaDB 5.1.x through 5.1.62, 5.2.x through 5.2.12, 5.3.x through 5.3.7, and 5.5.x through 5.5.25, allow remote authenticated users to execute arbitrary SQL commands via vectors related to the binary log. NOTE: as of 20130116, Oracle has not commented on claims from a downstream vendor that the fix in MySQL 5.5.29 is incomplete.

CVSS: 6.5

1.158 CVE-2014-2444

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.159 CVE-2014-2484

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.160 CVE-2015-2617

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.161 CVE-2012-3147

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote attackers to affect integrity and availability, related to MySQL Client.

CVSS: 6.4

1.162 CVE-2013-3798

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.163 CVE-2017-3454

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.164 CVE-2017-3455

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.165 CVE-2019-2731

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.166 CVE-2013-1570

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.167 CVE-2020-1967

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.168 CVE-2016-3588

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.169 CVE-2021-2356

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.170 CVE-2008-4097

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: MySQL 5.0.51a allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are associated with symlinks within pathnames for subdirectories of the MySQL home data directory, which are followed when tables are created in the future. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-2079.

CVSS: 4.6

1.171 CVE-2014-0433

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.172 CVE-2016-0594

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.173 CVE-2015-3152

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Oracle MySQL before 5.7.3, Oracle MySQL Connector/C (aka libmysql-client) 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

1.174 CVE-2017-3467

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.175 CVE-2017-3650

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.176 CVE-2018-0735

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.177 CVE-2020-1971

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.178 CVE-2007-2583

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: The in_decimal::set function in item_cmpfunc.cc in MySQL before 5.0.40, and 5.1 before 5.1.18-beta, allows context-dependent attackers to cause a denial of service (crash) via a crafted IF clause that results in a divide-by-zero error and a NULL pointer dereference.

CVSS: 4.0

1.179 CVE-2009-4019

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: mysqld in MySQL 5.0.x before 5.0.88 and 5.1.x before 5.1.41 does not (1) properly handle errors during execution of certain SELECT statements with subqueries, and does not (2) preserve certain null_value flags during execution of statements that use the GeomFromWKB function, which allows remote authenticated users to cause a denial of service (daemon crash) via a crafted statement.

CVSS: 4.0

1.180 CVE-2012-0583

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.60 and earlier, and 5.5.19 and earlier, allows remote authenticated users to affect availability, related to MyISAM.

CVSS: 4.0

1.181 CVE-2012-1696

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.19 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.

CVSS: 4.0

1.182 CVE-2012-3144

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server.

CVSS: 4.0

1.183 CVE-2013-3795

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.184 CVE-2013-3796

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.185 CVE-2013-3806

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.186 CVE-2013-3807

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.187 CVE-2013-5767

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.188 CVE-2013-5786

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.189 CVE-2013-5894

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.190 CVE-2013-5881

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.191 CVE-2014-2434

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.192 CVE-2014-2435

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.193 CVE-2014-2442

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.194 CVE-2014-2450

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.195 CVE-2014-4233

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.196 CVE-2014-4238

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.197 CVE-2015-0409

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.198 CVE-2015-0405

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.199 CVE-2015-0423

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.200 CVE-2015-0438

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.201 CVE-2015-0439

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.202 CVE-2015-0500

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.203 CVE-2015-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.204 CVE-2015-0508

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.205 CVE-2015-2611

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

CVSS: 4.0

1.206 CVE-2015-4756

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.207 CVE-2015-4772

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.208 CVE-2015-4730

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.209 CVE-2015-4800

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.210 CVE-2015-4833

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.211 CVE-2015-4862

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.212 CVE-2015-4904

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.213 CVE-2015-4905

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.214 CVE-2016-0503

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.215 CVE-2016-0595

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.216 CVE-2016-0611

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.217 CVE-2016-0616

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.

CVSS: 4.0

1.218 CVE-2016-3424

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.219 CVE-2016-3440

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.220 CVE-2016-5436

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.221 CVE-2016-5437

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.222 CVE-2016-5441

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.223 CVE-2016-5442

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.224 CVE-2016-5628

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.225 CVE-2016-5631

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.226 CVE-2016-5632

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.227 CVE-2016-5633

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.228 CVE-2016-5634

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.229 CVE-2016-5635

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.230 CVE-2017-3251

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.231 CVE-2017-3256

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.232 CVE-2017-3452

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.233 CVE-2017-3457

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.234 CVE-2017-3458

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.235 CVE-2017-3459

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.236 CVE-2017-3460

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.237 CVE-2017-3465

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.238 CVE-2017-3638

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.239 CVE-2017-3639

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.240 CVE-2017-3640

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.241 CVE-2017-3642

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.242 CVE-2017-3643

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.243 CVE-2017-3644

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.244 CVE-2017-3645

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.245 CVE-2017-3646

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.246 CVE-2017-10165

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.247 CVE-2017-10167

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.248 CVE-2017-10284

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.249 CVE-2017-10296

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.250 CVE-2017-10311

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.251 CVE-2017-10313

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.252 CVE-2018-3061

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.253 CVE-2018-3071

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.254 CVE-2019-2755

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.255 CVE-2019-2757

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.256 CVE-2022-21417

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.257 CVE-2014-4240

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.258 CVE-2010-2008

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: MySQL before 5.1.48 allows remote authenticated users with alter database privileges to cause a denial of service (server crash and database loss) via an ALTER DATABASE command with a #mysql50# string followed by a . (dot), .. (dot dot), ../ (dot dot slash) or similar sequence, and an UPGRADE DATA DIRECTORY NAME command, which causes MySQL to move certain directories to the server data directory.

CVSS: 3.5

1.259 CVE-2012-3149

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.26 and earlier allows remote authenticated users to affect confidentiality, related to MySQL Client.

CVSS: 3.5

1.260 CVE-2012-3156

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server.

CVSS: 3.5

1.261 CVE-2013-1566

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.262 CVE-2013-1567

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.263 CVE-2013-2381

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.264 CVE-2013-3810

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.265 CVE-2013-3811

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.266 CVE-2013-5793

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.267 CVE-2014-0427

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.268 CVE-2014-0431

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.269 CVE-2014-2451

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.270 CVE-2015-0385

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.271 CVE-2015-0506

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.272 CVE-2015-0507

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.273 CVE-2015-2567

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.274 CVE-2015-2639

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.275 CVE-2015-2641

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.276 CVE-2015-4761

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.277 CVE-2015-4769

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*
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

1.278 CVE-2015-4771

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.279 CVE-2015-4791

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.280 CVE-2015-4890

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.281 CVE-2016-0610

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.282 CVE-2016-0652

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.283 CVE-2016-0653

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.284 CVE-2016-0654

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.285 CVE-2016-0656

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.286 CVE-2016-0657

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.287 CVE-2016-0658

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.288 CVE-2016-0659

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.289 CVE-2016-0662

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.290 CVE-2016-0663

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.291 CVE-2016-8286

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.292 CVE-2016-8287

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.293 CVE-2016-8290

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.294 CVE-2017-3319

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.295 CVE-2017-3320

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.296 CVE-2017-3468

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.297 CVE-2017-3529

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.298 CVE-2017-3637

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.299 CVE-2019-2741

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.300 CVE-2014-4214

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.301 CVE-2016-8289

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.302 CVE-2014-0430

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.303 CVE-2015-0511

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.304 CVE-2015-2566

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.305 CVE-2016-0607

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.306 CVE-2016-0667

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.307 CVE-2019-7317

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.308 CVE-2012-4452

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

Summary: MySQL 5.0.88, and possibly other versions and platforms, allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL data home directory, related to incorrect calculation of the mysql_unpacked_real_data_home value. NOTE: this vulnerability exists because of a CVE-2009-4030 regression, which was not omitted in other packages and versions such as MySQL 5.0.95 in Red Hat Enterprise Linux 6.

CVSS: 2.1

1.309 CVE-2013-5770

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.310 CVE-2015-2661

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.311 CVE-2015-4910

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.312 CVE-2020-15358

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.313 CVE-2021-22570

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.314 CVE-2022-21444

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.315 CVE-2015-4766

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.316 CVE-2015-0498

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.317 CVE-2015-4767

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.318 CVE-2016-5443

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.319 CVE-2023-21977

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.320 CVE-2023-21980

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.321 CVE-2023-22007

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.322 CVE-2023-22015

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.323 CVE-2023-22026

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.324 CVE-2023-22028

!–> CVE for cpe:2.3:a:oracle:mysql:5.0.51a:::::*

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

1.325 CVE-2013-1902

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL, 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 generates insecure temporary files with predictable filenames, which has unspecified impact and attack vectors related to “graphical installers for Linux and Mac OS X.”

CVSS: 10.0

1.326 CVE-2013-1903

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL, possibly 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, 8.4.x before 8.4.17, and 8.3.x before 8.3.23 incorrectly provides the superuser password to scripts related to "graphical installers for Linux and Mac OS X," which has unspecified impact and attack vectors.

CVSS: 10.0

1.327 CVE-2016-7048

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The interactive installer in PostgreSQL before 9.3.15, 9.4.x before 9.4.10, and 9.5.x before 9.5.5 might allow remote attackers to execute arbitrary code by leveraging use of HTTP to download software.

CVSS: 9.3

1.328 CVE-2010-1169

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 does not properly restrict PL/perl procedures, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Perl code via a crafted script, related to the Safe module (aka Safe.pm) for Perl. NOTE: some sources report that this issue is the same as CVE-2010-1447.

CVSS: 8.5

1.329 CVE-2010-1447

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The Safe (aka Safe.pm) module 2.26, and certain earlier versions, for Perl, as used in PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2, allows context-dependent attackers to bypass intended (1) Safe::reval and (2) Safe::rdo access restrictions, and inject and execute arbitrary code, via vectors involving subroutine references and delayed execution.

CVSS: 8.5

1.330 CVE-2019-10211

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via bundled OpenSSL executing code from unprotected directory.

CVSS: 7.5

1.331 CVE-2015-3166

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The snprintf implementation in PostgreSQL before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 does not properly handle system-call errors, which allows attackers to obtain sensitive information or have other unspecified impact via unknown vectors, as demonstrated by an out-of-memory error.

CVSS: 7.5

1.332 CVE-2015-0244

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL before 9.0.19, 9.1.x before 9.1.15, 9.2.x before 9.2.10, 9.3.x before 9.3.6, and 9.4.x before 9.4.1 does not properly handle errors while reading a protocol message, which allows remote attackers to conduct SQL injection attacks via crafted binary data in a parameter and causing an error, which triggers the loss of synchronization and part of the protocol message to be treated as a new message, as demonstrated by causing a timeout or query cancellation.

CVSS: 7.5

1.333 CVE-2017-14798

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: A race condition in the postgresql init script could be used by attackers able to access the postgresql account to escalate their privileges to root.

CVSS: 6.9

1.334 CVE-2009-3231

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The core server component in PostgreSQL 8.3 before 8.3.8 and 8.2 before 8.2.14, when using LDAP authentication with anonymous binds, allows remote attackers to bypass authentication via an empty password.

CVSS: 6.8

1.335 CVE-2012-0868

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: CRLF injection vulnerability in pg_dump in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows user-assisted remote attackers to execute arbitrary SQL commands via a crafted file containing object names with newlines, which are inserted into an SQL script that is used when the database is restored.

CVSS: 6.8

1.336 CVE-2013-0255

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL 9.2.x before 9.2.3, 9.1.x before 9.1.8, 9.0.x before 9.0.12, 8.4.x before 8.4.16, and 8.3.x before 8.3.23 does not properly declare the enum_recv function in backend/utils/adt/enum.c, which causes it to be invoked with incorrect arguments and allows remote authenticated users to cause a denial of service (server crash) or read sensitive process memory via a crafted SQL command, which triggers an array index error and an out-of-bounds read.

CVSS: 6.8

1.337 CVE-2013-4422

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: SQL injection vulnerability in Quassel IRC before 0.9.1, when Qt 4.8.5 or later and PostgreSQL 8.2 or later are used, allows remote attackers to execute arbitrary SQL commands via a (backslash) in a message.

CVSS: 6.8

1.338 CVE-2020-25694

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVSS: 6.8

1.339 CVE-2009-3230

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, 8.2 before 8.2.14, 8.1 before 8.1.18, 8.0 before 8.0.22, and 7.4 before 7.4.26 does not use the appropriate privileges for the (1) RESET ROLE and (2) RESET SESSION AUTHORIZATION operations, which allows remote authenticated users to gain privileges. NOTE: this is due to an incomplete fix for CVE-2007-6600.

CVSS: 6.5

1.340 CVE-2009-4136

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly manage session-local state during execution of an index function by a database superuser, which allows remote authenticated users to gain privileges via a table with crafted index functions, as demonstrated by functions that modify (1) search_path or (2) a prepared statement, a related issue to CVE-2007-6600 and CVE-2009-3230.

CVSS: 6.5

1.341 CVE-2010-0442

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The bitsubstr function in backend/utils/adt/varbit.c in PostgreSQL 8.0.23, 8.1.11, and 8.3.8 allows remote authenticated users to cause a denial of service (daemon crash) or have unspecified other impact via vectors involving a negative integer in the third argument, as demonstrated by a SELECT statement that contains a call to the substring function for a bit string, related to an "overflow."

CVSS: 6.5

1.342 CVE-2010-4015

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Buffer overflow in the gettoken function in contrib/intarray/_int_bool.c in the intarray array module in PostgreSQL 9.0.x before 9.0.3, 8.4.x before 8.4.7, 8.3.x before 8.3.14, and 8.2.x before 8.2.20 allows remote authenticated users to cause a denial of service (crash) and possibly execute arbitrary code via integers with a large number of digits to unspecified functions.

CVSS: 6.5

1.343 CVE-2012-0866

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: CREATE TRIGGER in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 does not properly check the execute permission for trigger functions marked SECURITY DEFINER, which allows remote authenticated users to execute otherwise restricted triggers on arbitrary data by installing the trigger on an attacker-owned table.

CVSS: 6.5

1.344 CVE-2014-0061

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The validator functions for the procedural languages (PLs) in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to gain privileges via a function that is (1) defined in another language or (2) not allowed to be directly called by the user due to permissions.

CVSS: 6.5

1.345 CVE-2014-0063

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Multiple stack-based buffer overflows in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via vectors related to an incorrect MAXDATELEN constant and datetime values

involving (1) intervals, (2) timestamps, or (3) timezones, a different vulnerability than CVE-2014-0065.

CVSS: 6.5

1.346 CVE-2014-0064

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Multiple integer overflows in the path_in and other unspecified functions in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to have unspecified impact and attack vectors, which trigger a buffer overflow. NOTE: this identifier has been SPLIT due to different affected versions; use CVE-2014-2669 for the hstore vector.

CVSS: 6.5

1.347 CVE-2014-0065

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Multiple buffer overflows in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to have unspecified impact and attack vectors, a different vulnerability than CVE-2014-0063.

CVSS: 6.5

1.348 CVE-2016-5423

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 allow remote authenticated users to cause a denial of service (NULL pointer dereference and server crash), obtain sensitive memory information, or possibly execute arbitrary code via (1) a CASE expression within the test value subexpression of another CASE or (2) inlining of an SQL function that implements the equality operator used for a CASE expression involving values of different types.

CVSS: 6.5

1.349 CVE-2015-0241

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The to_char function in PostgreSQL before 9.0.19, 9.1.x before 9.1.15, 9.2.x before 9.2.10, 9.3.x before 9.3.6, and 9.4.x before 9.4.1 allows remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a (1) large number of digits when processing a numeric formatting template, which triggers a buffer over-read, or (2) crafted timestamp formatting template, which triggers a buffer overflow.

CVSS: 6.5

1.350 CVE-2015-0242

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Stack-based buffer overflow in the *printf function implementations in PostgreSQL before 9.0.19, 9.1.x before 9.1.15, 9.2.x before 9.2.10, 9.3.x before 9.3.6, and 9.4.x before 9.4.1, when running on a Windows system, allows remote authenticated users to cause a denial of service (crash) and possibly execute arbitrary code via a floating point number with a large precision, as demonstrated by using the to_char function.

CVSS: 6.5

1.351 CVE-2015-0243

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Multiple buffer overflows in contrib/pgcrypto in PostgreSQL before 9.0.19, 9.1.x before 9.1.15, 9.2.x before 9.2.10, 9.3.x before 9.3.6, and 9.4.x before 9.4.1 allow remote authenticated users to cause a denial of service (crash) and possibly execute arbitrary code via unspecified vectors.

CVSS: 6.5

1.352 CVE-2020-25695

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVSS: 6.5

1.353 CVE-2015-5288

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The crypt function in contrib/pgcrypto in PostgreSQL before 9.0.23, 9.1.x before 9.1.19, 9.2.x before 9.2.14, 9.3.x before 9.3.10, and 9.4.x before 9.4.5 allows attackers to cause a denial of service (server crash) or read arbitrary server memory via a "too-short" salt.

CVSS: 6.4

1.354 CVE-2018-1115

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: postgresql before versions 10.4, 9.6.9 is vulnerable in the adminpack extension, the pg_catalog.pg_logfile_rotate() function doesn't follow the same ACLs than pg_rorate_logfile. If the adminpack is added to a database, an attacker able to connect to it could exploit this to force log rotation.

CVSS: 6.4

1.355 CVE-2010-1170

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The PL/Tcl implementation in PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, 8.4 before 8.4.4, and 9.0 Beta before 9.0 Beta 2 loads Tcl code from the pltcl_modules table regardless of the table's ownership and permissions, which allows remote authenticated users, with database-creation privileges, to execute arbitrary Tcl code by creating this table and inserting a crafted Tcl script.

CVSS: 6.0

1.356 CVE-2010-3433

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The PL/perl and PL/Tcl implementations in PostgreSQL 7.4 before 7.4.30, 8.0 before 8.0.26, 8.1 before 8.1.22, 8.2 before 8.2.18, 8.3 before 8.3.12, 8.4 before 8.4.5, and 9.0 before 9.0.1 do not properly protect script execution by a different SQL user identity within the same session, which allows remote authenticated users to gain privileges via crafted script code in a SECURITY DEFINER function, as demonstrated by (1) redefining standard functions or (2) redefining operators, a different vulnerability than CVE-2010-1168, CVE-2010-1169, CVE-2010-1170, and CVE-2010-1447.

CVSS: 6.0

1.357 CVE-2009-4034

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL 7.4.x before 7.4.27, 8.0.x before 8.0.23, 8.1.x before 8.1.19, 8.2.x before 8.2.15, 8.3.x before 8.3.9, and 8.4.x before 8.4.2 does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based PostgreSQL servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended client-hostname restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

CVSS: 5.8

1.358 CVE-2010-1975

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL 7.4 before 7.4.29, 8.0 before 8.0.25, 8.1 before 8.1.21, 8.2 before 8.2.17, 8.3 before 8.3.11, and 8.4 before 8.4.4 does not properly check privileges during certain RESET ALL operations, which allows remote authenticated users to remove arbitrary parameter settings via a (1) ALTER USER or (2) ALTER DATABASE statement.

CVSS: 5.5

1.359 CVE-2021-23214

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: When the server is configured to use trust authentication with a clientcert requirement or to use cert authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of SSL certificate verification and encryption.

CVSS: 5.1

1.360 CVE-2011-2483

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.

CVSS: 5.0

1.361 CVE-2016-0773

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL before 9.1.20, 9.2.x before 9.2.15, 9.3.x before 9.3.11, 9.4.x before 9.4.6, and 9.5.x before 9.5.1 allows remote attackers to cause a denial of service (infinite loop or buffer overflow and crash) via a large Unicode character range in a regular expression.

CVSS: 5.0

1.362 CVE-2017-7484

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: It was found that some selectivity estimation functions in PostgreSQL before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3 did not check user privileges before providing information from pg_statistic, possibly leaking information. An unprivileged attacker could use this flaw to steal some information from tables they are otherwise not allowed to access.

CVSS: 5.0

1.363 CVE-2016-0768

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL PL/Java after 9.0 does not honor access controls on large objects.

CVSS: 5.0

1.364 CVE-2015-3167

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: contrib/pgcrypto in PostgreSQL before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 uses different error responses when an incorrect key is used, which makes it easier for attackers to obtain the key via a brute force attack.

CVSS: 5.0

1.365 CVE-2012-3488

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The libxslt support in contrib/xml2 in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 does not properly restrict access to files and URLs, which allows remote authenticated users to modify data, obtain sensitive information, or trigger outbound traffic to arbitrary external hosts by leveraging (1) stylesheet commands that are permitted by the libxslt security options or (2) an xslt_process feature, related to an XML External Entity (aka XXE) issue.

CVSS: 4.9

1.366 CVE-2014-0062

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Race condition in the (1) CREATE INDEX and (2) unspecified ALTER TABLE commands in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allows remote authenticated users to create an unauthorized index or read portions of unauthorized tables by creating or deleting a table with the same name during the timing window.

CVSS: 4.9

1.367 CVE-2014-0067

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The “make check” command for the test suites in PostgreSQL 9.3.3 and earlier does not properly invoke initdb to specify the authentication requirements for a database cluster to be used for the tests, which allows local users to gain privileges by leveraging access to this cluster.

CVSS: 4.6

1.368 CVE-2016-5424

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 might allow remote authenticated users with the CREATEDB or CREATEROLE role to gain superuser privileges via a (1) ” (double quote), (2) (backslash), (3) carriage return, or (4) newline character in a (a) database or (b) role name that is mishandled during an administrative operation.

CVSS: 4.6

1.369 CVE-2012-2143

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.

CVSS: 4.3

1.370 CVE-2015-3165

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Double free vulnerability in PostgreSQL before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 allows remote attackers to cause a denial of service (crash) by closing an SSL session at a time when the authentication timeout will expire during the session shutdown sequence.

CVSS: 4.3

1.371 CVE-2019-10127

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: A vulnerability was found in postgresql versions 11.x prior to 11.3. The Windows installer for BigSQL-supplied PostgreSQL does not lock down the ACL of the binary installation directory or the ACL of the data directory; it keeps the inherited ACL. In the default configuration, an attacker having both an unprivileged Windows account and an unprivileged PostgreSQL account can cause the PostgreSQL service account to execute arbitrary code. An attacker having only the unprivileged Windows account can read arbitrary data directory files, essentially bypassing database-imposed read access limitations. An attacker having only the unprivileged Windows account can also delete certain data directory files.

CVSS: 4.3

1.372 CVE-2019-10128

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: A vulnerability was found in postgresql versions 11.x prior to 11.3. The Windows installer for EnterpriseDB-supplied PostgreSQL does not lock down the ACL of the binary installation directory or the ACL of the data directory; it keeps the inherited ACL. In the default configuration, this allows a local attacker to read arbitrary data directory files, essentially bypassing database-imposed read access limitations. In plausible non-default configurations, an attacker having both an unprivileged Windows account and an unprivileged PostgreSQL account can cause the PostgreSQL service account to execute arbitrary code.

CVSS: 4.1

1.373 CVE-2009-3229

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The core server component in PostgreSQL 8.4 before 8.4.1, 8.3 before 8.3.8, and 8.2 before 8.2.14 allows remote authenticated users to cause a denial of service (backend shutdown) by “re-LOAD-ing” libraries from a certain plugins directory.

CVSS: 4.0

1.374 CVE-2012-2655

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL 8.3.x before 8.3.19, 8.4.x before 8.4.12, 9.0.x before 9.0.8, and 9.1.x before 9.1.4 allows remote authenticated users to cause a denial of service (server

crash) by adding the (1) SECURITY DEFINER or (2) SET attributes to a procedural language's call handler.

CVSS: 4.0

1.375 CVE-2012-3489

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The xml_parse function in the libxml2 support in the core server component in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 allows remote authenticated users to determine the existence of arbitrary files or URLs, and possibly obtain file or URL content that triggers a parsing error, via an XML value that refers to (1) a DTD or (2) an entity, related to an XML External Entity (aka XXE) issue.

CVSS: 4.0

1.376 CVE-2014-0060

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 does not properly enforce the ADMIN OPTION restriction, which allows remote authenticated members of a role to add or remove arbitrary users to that role by calling the SET ROLE command before the associated GRANT command.

CVSS: 4.0

1.377 CVE-2014-0066

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: The chkpass extension in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 does not properly check the return value of the crypt library function, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via unspecified vectors.

CVSS: 4.0

1.378 CVE-2014-8161

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: PostgreSQL before 9.0.19, 9.1.x before 9.1.15, 9.2.x before 9.2.10, 9.3.x before 9.3.6, and 9.4.x before 9.4.1 allows remote authenticated users to obtain sensitive column values by triggering constraint violation and then reading the error message.

CVSS: 4.0

1.379 CVE-2010-0733

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Integer overflow in src/backend/executor/nodeHash.c in PostgreSQL 8.4.1 and earlier, and 8.5 through 8.5alpha2, allows remote authenticated users to cause a denial

of service (daemon crash) via a SELECT statement with many LEFT JOIN clauses, related to certain hashtable size calculations.

CVSS: 3.5

1.380 CVE-2021-3393

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: An information leak was discovered in postgresql in versions before 13.2, before 12.6 and before 11.11. A user having UPDATE permission but not SELECT permission to a particular column could craft queries which, under some circumstances, might disclose values from that column in error messages. An attacker could use this flaw to obtain information stored in a column they are allowed to write but not read.

CVSS: 3.5

1.381 CVE-2019-10210

!–> CVE for cpe:2.3:a:postgresql:postgresql:8.3.1:::::*

Summary: Postgresql Windows installer before versions 11.5, 10.10, 9.6.15, 9.5.19, 9.4.24 is vulnerable via superuser writing password to unprotected temporary file.

CVSS: 1.9

1.382 CVE-2002-1511

!–> CVE for cpe:2.3:a:att:vnc:3.3.3:::::*

Summary: The vncserver wrapper for vnc before 3.3.3r2-21 uses the rand() function instead of srand(), which causes vncserver to generate weak cookies.

CVSS: 5.0

1.383 CVE-2002-0493

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat may be started without proper security settings if errors are encountered while reading the web.xml file, which could allow attackers to bypass intended restrictions.

CVSS: 7.5

1.384 CVE-2009-3548

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: The Windows installer for Apache Tomcat 6.0.0 through 6.0.20, 5.5.0 through 5.5.28, and possibly earlier versions uses a blank default password for the administrative user, which allows remote attackers to gain privileges.

CVSS: 7.5

1.385 CVE-2013-2185

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: The readObject method in the DiskFileItem class in Apache Tomcat and JBoss Web, as used in Red Hat JBoss Enterprise Application Platform 6.1.0 and Red

Hat JBoss Portal 6.0.0, allows remote attackers to write to arbitrary files via a NULL byte in a file name in a serialized instance, a similar issue to CVE-2013-2186. NOTE: this issue is reportedly disputed by the Apache Tomcat team, although Red Hat considers it a vulnerability. The dispute appears to regard whether it is the responsibility of applications to avoid providing untrusted data to be deserialized, or whether this class should inherently protect against this issue

CVSS: 7.5

1.386 CVE-2020-8022

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: A Incorrect Default Permissions vulnerability in the packaging of tomcat on SUSE Enterprise Storage 5, SUSE Linux Enterprise Server 12-SP2-BCL, SUSE Linux Enterprise Server 12-SP2-LTSS, SUSE Linux Enterprise Server 12-SP3-BCL, SUSE Linux Enterprise Server 12-SP3-LTSS, SUSE Linux Enterprise Server 12-SP4, SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 12-SP2, SUSE Linux Enterprise Server for SAP 12-SP3, SUSE Linux Enterprise Server for SAP 15, SUSE OpenStack Cloud 7, SUSE OpenStack Cloud 8, SUSE OpenStack Cloud Crowbar 8 allows local attackers to escalate from group tomcat to root. This issue affects: SUSE Enterprise Storage 5 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP2-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-BCL tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP3-LTSS tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server 12-SP4 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 12-SP5 tomcat versions prior to 9.0.35-3.39.1. SUSE Linux Enterprise Server 15-LTSS tomcat versions prior to 9.0.35-3.57.3. SUSE Linux Enterprise Server for SAP 12-SP2 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 12-SP3 tomcat versions prior to 8.0.53-29.32.1. SUSE Linux Enterprise Server for SAP 15 tomcat versions prior to 9.0.35-3.57.3. SUSE OpenStack Cloud 7 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud 8 tomcat versions prior to 8.0.53-29.32.1. SUSE OpenStack Cloud Crowbar 8 tomcat versions prior to 8.0.53-29.32.1.

CVSS: 7.2

1.387 CVE-2003-0044

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Multiple cross-site scripting (XSS) vulnerabilities in the (1) examples and (2) ROOT web applications for Jakarta Tomcat 3.x through 3.3.1a allow remote attackers to insert arbitrary web script or HTML.

CVSS: 6.8

1.388 CVE-2013-6357

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Cross-site request forgery (CSRF) vulnerability in the Manager application in Apache Tomcat 5.5.25 and earlier allows remote attackers to hijack the authentication of administrators for requests that manipulate application deployment via the POST

method, as demonstrated by a /manager/html/undeploy?path= URI. NOTE: the vendor disputes the significance of this report, stating that "the Apache Tomcat Security team has not accepted any reports of CSRF attacks against the Manager application … as they require a reckless system administrator.

CVSS: 6.8

1.389 CVE-2013-4444

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Unrestricted file upload vulnerability in Apache Tomcat 7.x before 7.0.40, in certain situations involving outdated java.io.File code and a custom JMX configuration, allows remote attackers to execute arbitrary code by uploading and accessing a JSP file.

CVSS: 6.8

1.390 CVE-2013-4286

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090.

CVSS: 5.8

1.391 CVE-2002-1148

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: The default servlet (org.apache.catalina.servlets.DefaultServlet) in Tomcat 4.0.4 and 4.1.10 and earlier allows remote attackers to read source code for server files via a direct request to the servlet.

CVSS: 5.0

1.392 CVE-2002-1895

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: The servlet engine in Jakarta Apache Tomcat 3.3 and 4.0.4, when using IIS and the ajp1.3 connector, allows remote attackers to cause a denial of service (crash) via a large number of HTTP GET requests for an MS-DOS device such as AUX, LPT1, CON, or PRN.

CVSS: 5.0

1.393 CVE-2002-2006

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: The default installation of Apache Tomcat 4.0 through 4.1 and 3.0 through 3.3.1 allows remote attackers to obtain the installation path and other sensitive system information via the (1) SnoopServlet or (2) TroubleShooter example servlets.

CVSS: 5.0

1.394 CVE-2003-0042

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Jakarta Tomcat before 3.3.1a, when used with JDK 1.3.1 or earlier, allows remote attackers to list directories even with an index.html or other file present, or obtain unprocessed source code for a JSP file, via a URL containing a null character.

CVSS: 5.0

1.395 CVE-2003-0043

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Jakarta Tomcat before 3.3.1a, when used with JDK 1.3.1 or earlier, uses trusted privileges when processing the web.xml file, which could allow remote attackers to read portions of some files through the web.xml file.

CVSS: 5.0

1.396 CVE-2003-0045

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Jakarta Tomcat before 3.3.1a on certain Windows systems may allow remote attackers to cause a denial of service (thread hang and resource consumption) via a request for a JSP page containing an MS-DOS device name, such as aux.jsp.

CVSS: 5.0

1.397 CVE-2005-0808

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat before 5.x allows remote attackers to cause a denial of service (application crash) via a crafted AJP12 packet to TCP port 8007.

CVSS: 5.0

1.398 CVE-2008-0128

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: The SingleSignOn Valve (org.apache.catalina.authenticator.SingleSignOn) in Apache Tomcat before 5.5.21 does not set the secure flag for the JSESSIONIDSSO cookie in an https session, which can cause the cookie to be sent in http requests and make it easier for remote attackers to capture this cookie.

CVSS: 5.0

1.399 CVE-2014-0075

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Integer overflow in the parseChunkHeader function in java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 allows remote attackers to cause a denial of service (resource

consumption) via a malformed chunk size in chunked transfer coding of a request during the streaming of data.

CVSS: 5.0

1.400 CVE-2005-4838

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Multiple cross-site scripting (XSS) vulnerabilities in the example web applications for Jakarta Tomcat 5.5.6 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) el/functions.jsp, (2) el/implicit-objects.jsp, and (3) jspx/textRotate.jspx in examples/jsp2/, as demonstrated via script in a request to snp/snoop.jsp. NOTE: other XSS issues in the manager were simultaneously reported, but these require admin access and do not cross privilege boundaries.

CVSS: 4.3

1.401 CVE-2006-7196

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Cross-site scripting (XSS) vulnerability in the calendar application example in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.31, 5.0.0 through 5.0.30, and 5.5.0 through 5.5.15 allows remote attackers to inject arbitrary web script or HTML via the time parameter to cal2.jsp and possibly unspecified other vectors. NOTE: this may be related to CVE-2006-0254.1.

CVSS: 4.3

1.402 CVE-2007-2449

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Multiple cross-site scripting (XSS) vulnerabilities in certain JSP files in the examples web application in Apache Tomcat 4.0.0 through 4.0.6, 4.1.0 through 4.1.36, 5.0.0 through 5.0.30, 5.5.0 through 5.5.24, and 6.0.0 through 6.0.13 allow remote attackers to inject arbitrary web script or HTML via the portion of the URI after the ';' character, as demonstrated by a URI containing a "snp/snoop.jsp;" sequence.

CVSS: 4.3

1.403 CVE-2007-3384

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Multiple cross-site scripting (XSS) vulnerabilities in examples/servlet/CookieExample in Apache Tomcat 3.3 through 3.3.2 allow remote attackers to inject arbitrary web script or HTML via the (1) Name or (2) Value field, related to error messages.

CVSS: 4.3

1.404 CVE-2007-3382

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 treats single quotes ("'") as delimiters in cookies, which might

cause sensitive information such as session IDs to be leaked and allow remote attackers to conduct session hijacking attacks.

CVSS: 4.3

1.405 CVE-2007-3385

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat 6.0.0 to 6.0.13, 5.5.0 to 5.5.24, 5.0.0 to 5.0.30, 4.1.0 to 4.1.36, and 3.3 to 3.3.2 does not properly handle the " character sequence in a cookie value, which might cause sensitive information such as session IDs to be leaked to remote attackers and enable session hijacking attacks.

CVSS: 4.3

1.406 CVE-2009-2696

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Cross-site scripting (XSS) vulnerability in jsp/cal/cal2.jsp in the calendar application in the examples web application in Apache Tomcat on Red Hat Enterprise Linux 5, Desktop Workstation 5, and Linux Desktop 5 allows remote attackers to inject arbitrary web script or HTML via the time parameter, related to "invalid HTML." NOTE: this is due to a missing fix for CVE-2009-0781.

CVSS: 4.3

1.407 CVE-2013-4322

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 processes chunked transfer coding without properly handling (1) a large total amount of chunked data or (2) whitespace characters in an HTTP header value within a trailer field, which allows remote attackers to cause a denial of service by streaming data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3544.

CVSS: 4.3

1.408 CVE-2013-4590

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 allows attackers to obtain "Tomcat internals" information by leveraging the presence of an untrusted web application with a context.xml, web.xml, *.jspx,* .tagx, or *.tld XML document containing an external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

CVSS: 4.3

1.409 CVE-2014-0096

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: java/org/apache/catalina/servlets/DefaultServlet.java in the default servlet in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 does not properly restrict XSLT stylesheets, which allows remote attackers to bypass security-manager

restrictions and read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue.

CVSS: 4.3

1.410 CVE-2014-0099

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Integer overflow in java/org/apache/tomcat/util/buf/Ascii.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4, when operated behind a reverse proxy, allows remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header.

CVSS: 4.3

1.411 CVE-2014-0119

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Apache Tomcat before 6.0.40, 7.x before 7.0.54, and 8.x before 8.0.6 does not properly constrain the class loader that accesses the XML parser used with an XSLT stylesheet, which allows remote attackers to (1) read arbitrary files via a crafted web application that provides an XML external entity declaration in conjunction with an entity reference, related to an XML External Entity (XXE) issue, or (2) read files associated with different web applications on a single Tomcat instance via a crafted web application.

CVSS: 4.3

1.412 CVE-2007-1358

!–> CVE for cpe:2.3:a:apache:tomcat:3.3:::::*

Summary: Cross-site scripting (XSS) vulnerability in certain applications using Apache Tomcat 4.0.0 through 4.0.6 and 4.1.0 through 4.1.34 allows remote attackers to inject arbitrary web script or HTML via crafted “Accept-Language headers that do not conform to RFC 2616”.

CVSS: 2.6

1.413 CVE-2017-15698

!–> CVE for cpe:2.3:a:apache:tomcat_native:1.1.23:::::*

Summary: When parsing the AIA-Extension field of a client certificate, Apache Tomcat Native Connector 1.2.0 to 1.2.14 and 1.1.23 to 1.1.34 did not correctly handle fields longer than 127 bytes. The result of the parsing error was to skip the OCSP check. It was therefore possible for client certificates that should have been rejected (if the OCSP check had been made) to be accepted. Users not using OCSP checks are not affected by this vulnerability.

CVSS: 4.3

1.414 CVE-2018-8019

!–> CVE for cpe:2.3:a:apache:tomcat_native:1.1.23:::::*

Summary: When using an OCSP responder Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 did not correctly handle invalid responses. This allowed for revoked client certificates to be incorrectly identified. It was therefore possible for users to authenticate with revoked certificates when using mutual TLS. Users not using OCSP checks are not affected by this vulnerability.

CVSS: 4.3

1.415 CVE-2018-8020

!–> CVE for cpe:2.3:a:apache:tomcat_native:1.1.23:::::::*

Summary: Apache Tomcat Native 1.2.0 to 1.2.16 and 1.1.23 to 1.1.34 has a flaw that does not properly check OCSP pre-produced responses, which are lists (multiple entries) of certificate statuses. Subsequently, revoked client certificates may not be properly identified, allowing for users to authenticate with revoked certificates to connections that require mutual TLS. Users not using OCSP checks are not affected by this vulnerability.

CVSS: 4.3