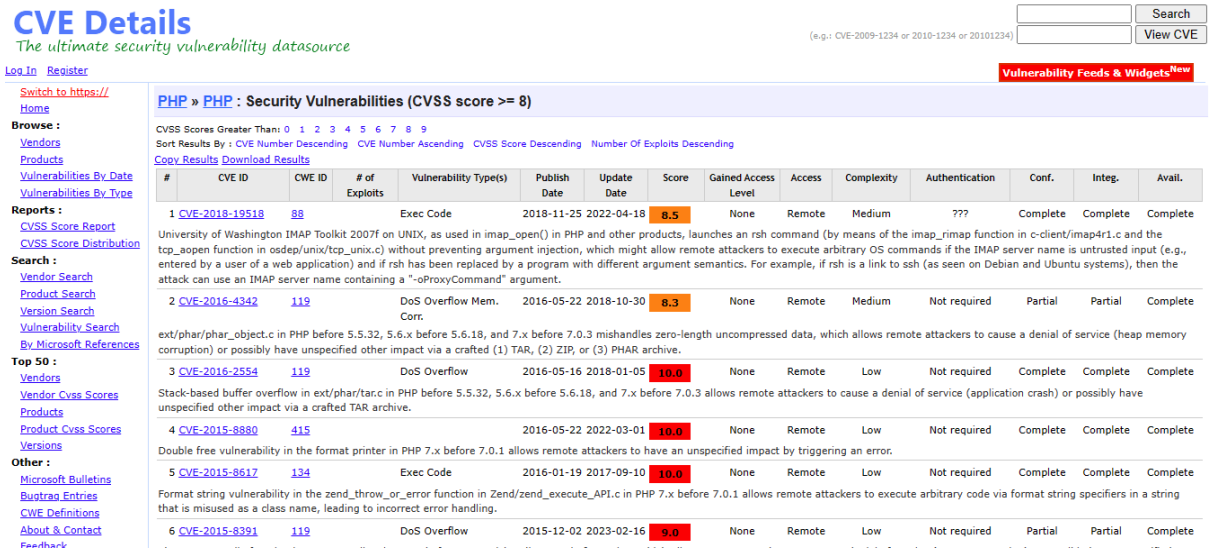
PHP 7.4.27 , 8.0.14 , 8.1.1 ค่า CVSS Score >=8 นั้นไม่มีอยู่ มีแต่ version อื่น



CVE Details
The ultimate security vulnerability datasource

Search / View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback

PHP » PHP : Security Vulnerabilities (CVSS score >= 8)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2018-19518	88		Exec Code	2018-11-25	2022-04-18	8.5	None	Remote	Medium	???	Complete	Complete	Complete

University of Washington IMAP Toolkit 2007f on UNIX, as used in imap_open() in PHP and other products, launches an rsh command (by means of the imap_rimap function in c-client/imap4r1.c and the tcp_aopen function in osdep/unix/tcp_unix.c) without preventing argument injection, which might allow remote attackers to execute arbitrary OS commands if the IMAP server name is untrusted input (e.g., entered by a user of a web application) and if rsh has been replaced by a program with different argument semantics. For example, if rsh is a link to ssh (as seen on Debian and Ubuntu systems), then the attack can use an IMAP server name containing a "-oProxyCommand" argument.

2	CVE-2016-4342	119		DoS Overflow Mem. Corr.	2016-05-22	2018-10-30	8.3	None	Remote	Medium	Not required	Partial	Partial	Complete

ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive.

3	CVE-2016-2554	119		DoS Overflow	2016-05-16	2018-01-05	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive.

4	CVE-2015-8880	415			2016-05-22	2022-03-01	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

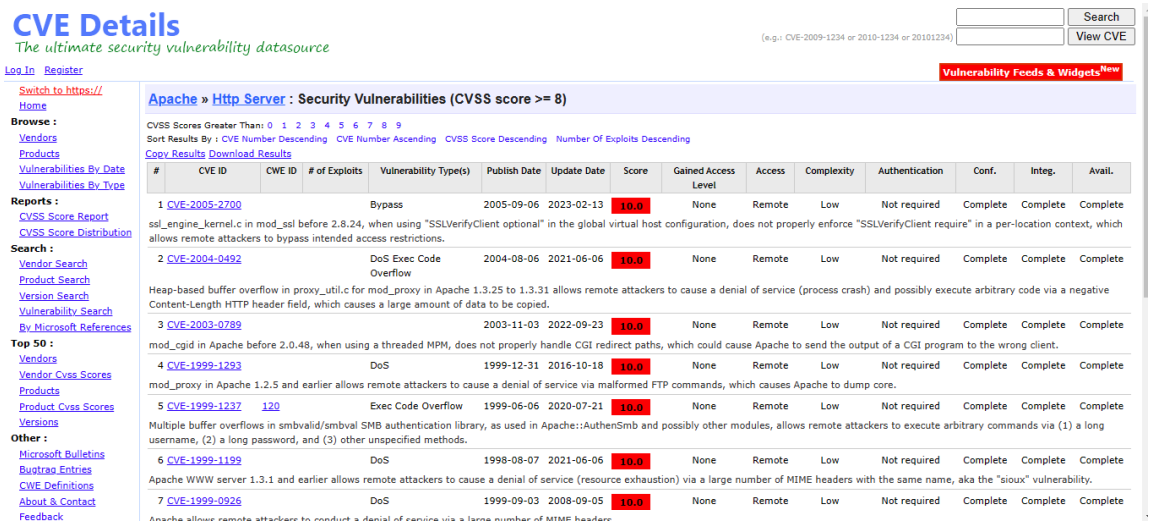
Double free vulnerability in the format printer in PHP 7.x before 7.0.1 allows remote attackers to have an unspecified impact by triggering an error.

5	CVE-2015-8617	134		Exec Code	2016-01-19	2017-09-10	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Format string vulnerability in the zend_throw_or_error function in Zend/zend_execute_API.c in PHP 7.x before 7.0.1 allows remote attackers to execute arbitrary code via format string specifiers in a string that is misused as a class name, leading to incorrect error handling.

6	CVE-2015-8391	119		DoS Overflow	2015-12-02	2023-02-16	9.0	None	Remote	Low	Not required	Partial	Partial	Complete

Apache 2.4.52 ค่า CVSS Score >=8 นั้นไม่มีอยู่ มีแต่ version อื่น



CVE Details
The ultimate security vulnerability datasource

Search / View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback

Apache » Http Server : Security Vulnerabilities (CVSS score >= 8)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2005-2700			Bypass	2005-09-06	2023-02-13	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

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.

2	CVE-2004-0492			DoS Exec Code Overflow	2004-08-06	2021-06-06	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Heap-based buffer overflow in proxy_util.c for mod_proxy in Apache 1.3.25 to 1.3.31 allows remote attackers to cause a denial of service (process crash) and possibly execute arbitrary code via a negative Content-Length HTTP header field, which causes a large amount of data to be copied.

3	CVE-2003-0789				2003-11-03	2022-09-23	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

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.

4	CVE-1999-1293			DoS	1999-12-31	2016-10-18	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

mod_proxy in Apache 1.2.5 and earlier allows remote attackers to cause a denial of service via malformed FTP commands, which causes Apache to dump core.

5	CVE-1999-1237	120		Exec Code Overflow	1999-06-06	2020-07-21	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Multiple buffer overflows in smbvalid/smbval SMB authentication library, as used in Apache::AuthenSmb and possibly other modules, allows remote attackers to execute arbitrary commands via (1) a long username, (2) a long password, and (3) other unspecified methods.

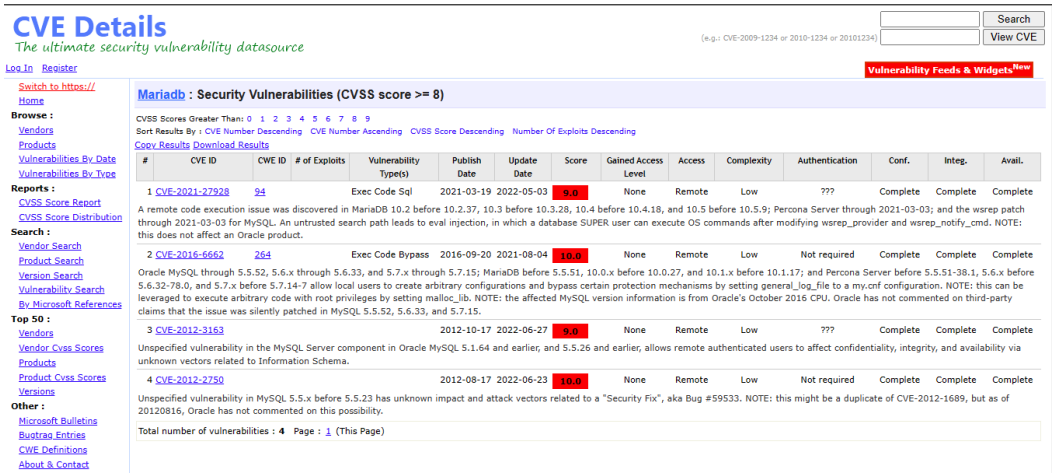
6	CVE-1999-1199			DoS	1998-08-07	2021-06-06	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Apache WWW server 1.3.1 and earlier allows remote attackers to cause a denial of service (resource exhaustion) via a large number of MIME headers with the same name, aka the "sioux" vulnerability.

7	CVE-1999-0926			DoS	1999-09-03	2008-09-05	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Apache allows remote attackers to conduct a denial of service via a large number of MIME headers

MariaDB 10.4.22 ค่า CVSS Score >=8 นั้นไม่มีอยู่ มีแต่ version อื่น



CVE Details
The ultimate security vulnerability datasource

Search / View CVE (e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

Log In Register

Vulnerability Feeds & Widgets New

Switch to https://
Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact

Mariadb : Security Vulnerabilities (CVSS score >= 8)

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2021-27928	94		Exec Code Sql	2021-03-19	2022-05-03	9.0	None	Remote	Low	???	Complete	Complete	Complete

A remote code execution issue was discovered in MariaDB 10.2 before 10.2.37, 10.3 before 10.3.28, 10.4 before 10.4.18, and 10.5 before 10.5.9; Percona Server through 2021-03-03; and the wsrep patch through 2021-03-03 for MySQL. An untrusted search path leads to eval injection, in which a database SUPER user can execute OS commands after modifying wsrep_provider and wsrep_notify_cmd. NOTE: this does not affect an Oracle product.

2	CVE-2016-6662	264		Exec Code Bypass	2016-09-20	2021-08-04	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.

3	CVE-2012-3163				2012-10-17	2022-06-27	9.0	None	Remote	Low	???	Complete	Complete	Complete

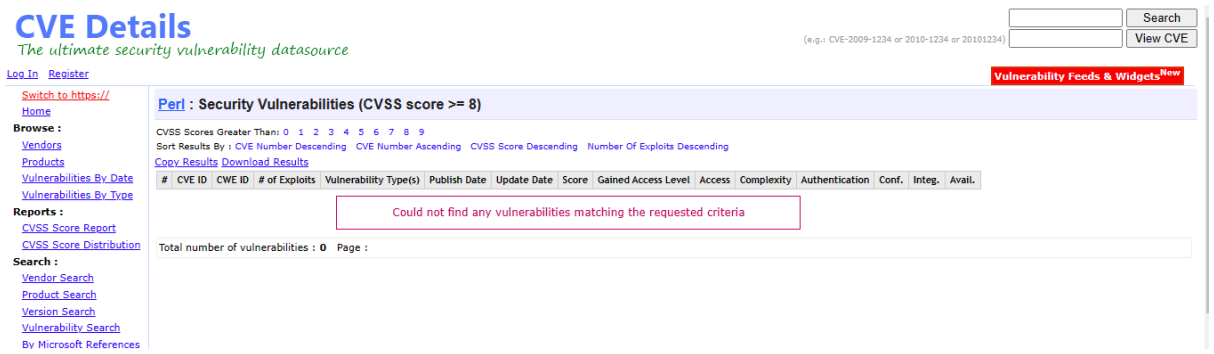
Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.64 and earlier, and 5.5.26 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Information Schema.

4	CVE-2012-2750				2012-08-17	2022-06-23	10.0	None	Remote	Low	Not required	Complete	Complete	Complete

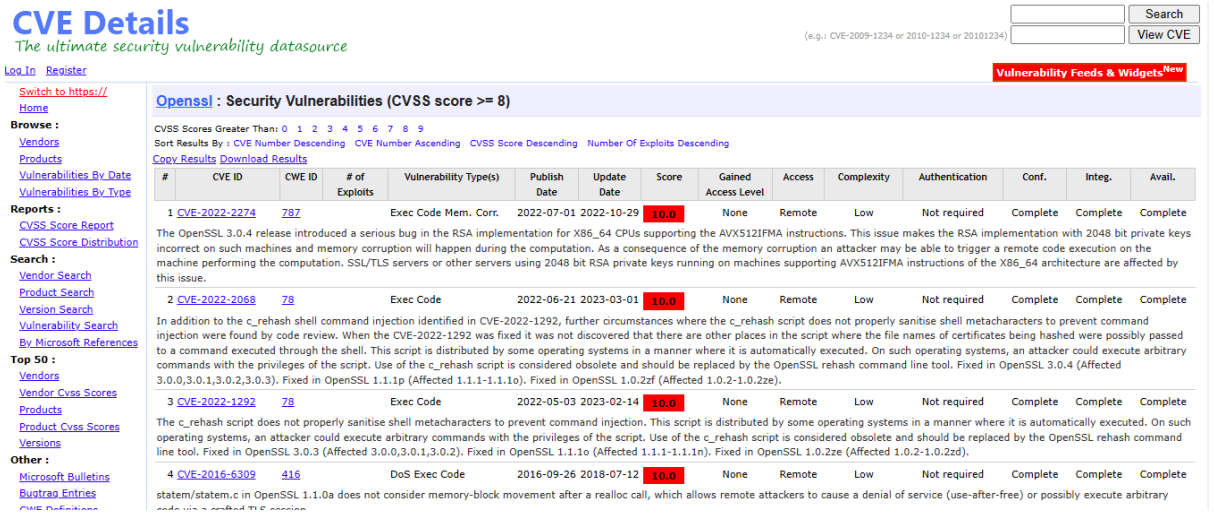
Unspecified vulnerability in MySQL 5.5.x before 5.5.23 has unknown impact and attack vectors related to a "Security Fix", aka Bug #59533. NOTE: this might be a duplicate of CVE-2012-1689, but as of 20120816, Oracle has not commented on this possibility.

Total number of vulnerabilities : 4 Page : 1 (This Page)

Perl 5.32.1 ค่า CVSS Score >=8 นั้นไม่มีอยู่



OpenSSL 1.1.1m (UNIX only) ค่า CVSS Score >=8 นั้นไม่มีอยู่ มีแต่ version อื่น



phpMyAdmin 5.1.1 ค่า CVSS Score >=8 นั้นไม่มีอยู่