



CVE-2012-2122

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-2122
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-06-26 18:55:00 UTC
Updated	2014-02-21 04:50:00 UTC
Description	sql/password.c in Oracle MySQL 5.1.x before 5.1.63, 5.5.x before 5.5.24, and 5.6.x before 5.6.6, and MariaDB 5.1.x before

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mariadb	Mariadb	5.1.41	All	All	All
Application	Mariadb	Mariadb	5.1.42	All	All	All
Application	Mariadb	Mariadb	5.1.44	All	All	All
Application	Mariadb	Mariadb	5.1.47	All	All	All
Application	Mariadb	Mariadb	5.1.49	All	All	All
Application	Mariadb	Mariadb	5.1.50	All	All	All
Application	Mariadb	Mariadb	5.1.51	All	All	All
Application	Mariadb	Mariadb	5.1.53	All	All	All
Application	Mariadb	Mariadb	5.1.55	All	All	All
Application	Mariadb	Mariadb	5.1.60	All	All	All
Application	Mariadb	Mariadb	5.1.61	All	All	All
Application	Mariadb	Mariadb	5.2.0	All	All	All
Application	Mariadb	Mariadb	5.2.1	All	All	All
Application	Mariadb	Mariadb	5.2.10	All	All	All
Application	Mariadb	Mariadb	5.2.11	All	All	All
Application	Mariadb	Mariadb	5.2.2	All	All	All
Application	Mariadb	Mariadb	5.2.3	All	All	All

Application	Mariadb	Mariadb	5.2.4	All	All	All
Application	Mariadb	Mariadb	5.2.5	All	All	All
Application	Mariadb	Mariadb	5.2.6	All	All	All
Application	Mariadb	Mariadb	5.2.7	All	All	All
Application	Mariadb	Mariadb	5.2.8	All	All	All
Application	Mariadb	Mariadb	5.2.9	All	All	All
Application	Mariadb	Mariadb	5.3.0	All	All	All
Application	Mariadb	Mariadb	5.3.1	All	All	All
Application	Mariadb	Mariadb	5.3.2	All	All	All
Application	Mariadb	Mariadb	5.3.3	All	All	All
Application	Mariadb	Mariadb	5.3.4	All	All	All
Application	Mariadb	Mariadb	5.3.5	All	All	All
Application	Mariadb	Mariadb	5.3.6	All	All	All
Application	Mariadb	Mariadb	5.5.20	All	All	All
Application	Mariadb	Mariadb	5.5.21	All	All	All
Application	Mariadb	Mariadb	5.5.22	All	All	All
Application	Mariadb	Mariadb	5.1.41	All	All	All
Application	Mariadb	Mariadb	5.1.42	All	All	All
Application	Mariadb	Mariadb	5.1.44	All	All	All
Application	Mariadb	Mariadb	5.1.47	All	All	All
Application	Mariadb	Mariadb	5.1.49	All	All	All
Application	Mariadb	Mariadb	5.1.50	All	All	All
Application	Mariadb	Mariadb	5.1.51	All	All	All
Application	Mariadb	Mariadb	5.1.53	All	All	All
Application	Mariadb	Mariadb	5.1.55	All	All	All
Application	Mariadb	Mariadb	5.1.60	All	All	All
Application	Mariadb	Mariadb	5.1.61	All	All	All
Application	Mariadb	Mariadb	5.2.0	All	All	All
Application	Mariadb	Mariadb	5.2.1	All	All	All
Application	Mariadb	Mariadb	5.2.10	All	All	All
Application	Mariadb	Mariadb	5.2.11	All	All	All
Application	Mariadb	Mariadb	5.2.2	All	All	All
Application	Mariadb	Mariadb	5.2.3	All	All	All
Application	Mariadb	Mariadb	5.2.4	All	All	All
Application	Mariadb	Mariadb	5.2.5	All	All	All

Application	Mariadb	Mariadb	5.2.6	All	All	All
Application	Mariadb	Mariadb	5.2.7	All	All	All
Application	Mariadb	Mariadb	5.2.8	All	All	All
Application	Mariadb	Mariadb	5.2.9	All	All	All
Application	Mariadb	Mariadb	5.3.0	All	All	All
Application	Mariadb	Mariadb	5.3.1	All	All	All
Application	Mariadb	Mariadb	5.3.2	All	All	All
Application	Mariadb	Mariadb	5.3.3	All	All	All
Application	Mariadb	Mariadb	5.3.4	All	All	All
Application	Mariadb	Mariadb	5.3.5	All	All	All
Application	Mariadb	Mariadb	5.3.6	All	All	All
Application	Mariadb	Mariadb	5.5.20	All	All	All
Application	Mariadb	Mariadb	5.5.21	All	All	All
Application	Mariadb	Mariadb	5.5.22	All	All	All
Application	Oracle	Mysql	5.1.51	All	All	All
Application	Oracle	Mysql	5.1.52	All	All	All
Application	Oracle	Mysql	5.1.52	sp1	All	All
Application	Oracle	Mysql	5.1.53	All	All	All
Application	Oracle	Mysql	5.1.54	All	All	All
Application	Oracle	Mysql	5.1.55	All	All	All
Application	Oracle	Mysql	5.1.56	All	All	All
Application	Oracle	Mysql	5.1.57	All	All	All
Application	Oracle	Mysql	5.1.58	All	All	All
Application	Oracle	Mysql	5.1.59	All	All	All
Application	Oracle	Mysql	5.1.60	All	All	All
Application	Oracle	Mysql	5.1.61	All	All	All
Application	Oracle	Mysql	5.5.10	All	All	All
Application	Oracle	Mysql	5.5.11	All	All	All
Application	Oracle	Mysql	5.5.12	All	All	All
Application	Oracle	Mysql	5.5.13	All	All	All
Application	Oracle	Mysql	5.5.14	All	All	All
Application	Oracle	Mysql	5.5.15	All	All	All
Application	Oracle	Mysql	5.5.16	All	All	All
Application	Oracle	Mysql	5.5.17	All	All	All
Application	Oracle	Mysql	5.5.18	All	All	All
Application	Oracle	Mysql	5.5.19	All	All	All

Application	Oracle	Mysql	5.5.19	All	All	All
Application	Oracle	Mysql	5.5.20	All	All	All
Application	Oracle	Mysql	5.5.21	All	All	All
Application	Oracle	Mysql	5.6.2	All	All	All
Application	Oracle	Mysql	5.6.3	All	All	All
Application	Oracle	Mysql	5.6.4	All	All	All
Application	Oracle	Mysql	5.6.5	All	All	All
Application	Oracle	Mysql	5.1.51	All	All	All
Application	Oracle	Mysql	5.1.52	All	All	All
Application	Oracle	Mysql	5.1.52	sp1	All	All
Application	Oracle	Mysql	5.1.53	All	All	All
Application	Oracle	Mysql	5.1.54	All	All	All
Application	Oracle	Mysql	5.1.55	All	All	All
Application	Oracle	Mysql	5.1.56	All	All	All
Application	Oracle	Mysql	5.1.57	All	All	All
Application	Oracle	Mysql	5.1.58	All	All	All
Application	Oracle	Mysql	5.1.59	All	All	All
Application	Oracle	Mysql	5.1.60	All	All	All
Application	Oracle	Mysql	5.1.61	All	All	All
Application	Oracle	Mysql	5.5.10	All	All	All
Application	Oracle	Mysql	5.5.11	All	All	All
Application	Oracle	Mysql	5.5.12	All	All	All
Application	Oracle	Mysql	5.5.13	All	All	All
Application	Oracle	Mysql	5.5.14	All	All	All
Application	Oracle	Mysql	5.5.15	All	All	All
Application	Oracle	Mysql	5.5.16	All	All	All
Application	Oracle	Mysql	5.5.17	All	All	All
Application	Oracle	Mysql	5.5.18	All	All	All
Application	Oracle	Mysql	5.5.19	All	All	All
Application	Oracle	Mysql	5.5.20	All	All	All
Application	Oracle	Mysql	5.5.21	All	All	All
Application	Oracle	Mysql	5.6.2	All	All	All
Application	Oracle	Mysql	5.6.3	All	All	All
Application	Oracle	Mysql	5.6.4	All	All	All
Application	Oracle	Mysql	5.6.5	All	All	All

References		
Reference	Source	Link
MySQL Bugs: #64884: logins with incorrect password are allowed	MISC	bugs.mysql.com
MySQL Remote Root Authentication Bypass	EXPLOIT-DB	www.exploit-db.com
Oracle MySQL CVE-2012-2122 User Login Security Bypass Vulnerability	BID	www.securityfocus.com
MySQL memcmp() Comparison Error Lets Remote Users Bypass Authentication - SecurityTracker	SECTrack	securitytracker.com
About Secunia Research Flexera	SECUNIA	secunia.com
oss-sec: Security vulnerability in MySQL/MariaDB sql/password.c	MLIST	seclists.org
Gentoo Linux Documentation -- MySQL: Multiple vulnerabilities	GENTOO	security.gentoo.org
CVE-2012-2122: A Tragically Comedic Security Flaw in MySQL	MISC	community.rapid7.com
Security Alerts - Secunia	SECUNIA	secunia.com
[security-announce] SUSE-SU-2012:0984-1: important: Security update for	SUSE	lists.opensuse.org
MariaDB 5.1.62 Release Notes - AskMonty KnowledgeBase	CONFIRM	kb.askmonty.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		

© [CVE.report](https://cve.report) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](https://mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://mitre.org). This site includes MITRE data granted under the following [license](https://mitre.org).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report