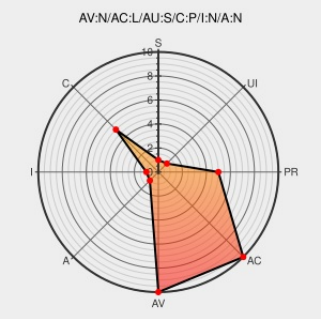
CVE-2012-5627

Published on: 10/01/2013 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:23 AM UTC

CVE-2012-5627

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mariadb from Mariadb contain the following vulnerability:

Oracle MySQL and MariaDB 5.5.x before 5.5.29, 5.3.x before 5.3.12, and 5.2.x before 5.2.14 does not modify the salt during multiple executions of the change_user command within the same connection which makes it easier for remote authenticated users to conduct brute force password guessing attacks.

CVE-2012-5627 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
oss-sec: Re: CVE request: Mysql/Mariadb insecure salt-usage	Mailing List, Third Party Advisory, seclists.org, text/html	MLIST [oss-security] 20121206 Re: CVE request: Mysql/Mariadb insecure salt-usage
Bug 883719 – CVE-2012-5627 mysql: efficient password guessing attack using change_user()	Issue Tracking, Patch, Third Party Advisory, bugzilla.redhat.com, text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=883719
[#MDEV-3915] COM_CHANGE_USER allows fast password brute-forcing - JIRA	Vendor Advisory, mariadb.atlassian.net, text/html	CONFIRM mariadb.atlassian.net/browse/MDEV-3915

About Secunia Research | Flexera	Not Applicable secunia.com Depreciated Link text/plain	SECUNIA 53372
Support / Security / Advisories / / MDVSA-2013:102 | Mandriva	Broken Link www.mandriva.com text/html	MANDRIVA MDVSA-2013:102
Full Disclosure: Re: MySQL Local/Remote FAST Account Password Cracking	Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20121205 Re: MySQL Local/Remote FAST Account Password Cracking
Gentoo Linux Documentation -- MySQL: Multiple vulnerabilities	Patch Third Party Advisory VDB Entry security.gentoo.org text/html	GENTOO GLSA-201308-06
Full Disclosure: MySQL Local/Remote FAST Account Password Cracking	Exploit Mailing List Third Party Advisory seclists.org text/html	FULLDISC 20121203 MySQL Local/Remote FAST Account Password Cracking

Related QID Numbers

900276 CBL-Mariner Linux Security Update for mysql 8.0.24

900307 CBL-Mariner Linux Security Update for mysql 8.0.26

901561 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (6692-1)

903310 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (2669)

906168 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (2669-1)

906449 Common Base Linux Mariner (CBL-Mariner) Security Update for mysql (6692-2)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mariadb	Mariadb	All	All	All	All
Application	Mariadb	Mariadb	10.0.0	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	5.2.12	All	All	All
Application	Mariadb	Mariadb	5.2.13	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	5.3.10	All	All	All
Application	Mariadb	Mariadb	5.3.11	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	5.3.7	All	All	All
Application	Mariadb	Mariadb	5.3.8	All	All	All
Application	Mariadb	Mariadb	5.3.9	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	5.5.23	All	All	All
Application	Mariadb	Mariadb	5.5.24	All	All	All
Application	Mariadb	Mariadb	5.5.25	All	All	All
Application	Mariadb	Mariadb	5.5.27	All	All	All
Application	Mariadb	Mariadb	5.5.28	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	5.2.12	All	All	All
Application	Mariadb	Mariadb	5.2.13	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	5.3.10	All	All	All
Application	Mariadb	Mariadb	5.3.11	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	5.3.7	All	All	All
Application	Mariadb	Mariadb	5.3.8	All	All	All
Application	Mariadb	Mariadb	5.3.9	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	5.5.23	All	All	All
Application	Mariadb	Mariadb	5.5.24	All	All	All
Application	Mariadb	Mariadb	5.5.25	All	All	All
Application	Mariadb	Mariadb	5.5.27	All	All	All
Application	Mariadb	Mariadb	5.5.28	All	All	All
Application	Mysql	Mysql	All	All	All	All
Application	Mysql	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All

cpe:2.3:a:mariadb:mariadb:*:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:10.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.10:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.11:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.12:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.13:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.2:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.3:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.4:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.5:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.6:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.7:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.8:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.2.9:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.0:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.1:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.10:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.11:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.2:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.3:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.4:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.5:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.6:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.7:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.8:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.3.9:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.5.20:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.5.21:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.5.22:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.5.23:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.5.24:*:*:*:*:*:*:*

cpe:2.3:a:mariadb:mariadb:5.5.25:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.27:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.28:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.10:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.11:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.12:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.13:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.4:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.5:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.6:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.7:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.8:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.2.9:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.10:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.11:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.2:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.3:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.4:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.5:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.6:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.7:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.8:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.3.9:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.20:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.21:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.22:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.23:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.24:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.25:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.27:*:*:*:*:*:*:*:

cpe:2.3:a:mariadb:mariadb:5.5.28:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→