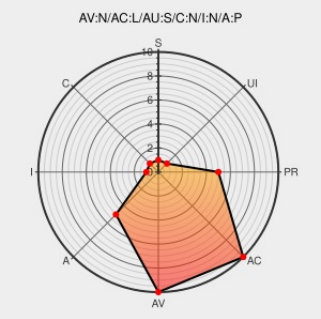
CVE-2012-5614

Published on: 12/03/2012 12:00:00 AM UTC

Last Modified on: 08/29/2022 08:56:00 PM UTC

CVE-2012-5614

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



Certain versions of Mariadb from Mariadb contain the following vulnerability:

Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier, and MariaDB 5.5.28a and possibly other versions, allows remote authenticated users to cause a denial of service (mysqld crash) via a SELECT command with an UpdateXML command containing XML with a large number of unique, nested elements.

CVE-2012-5614 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**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
Oracle Critical Patch Update - April 2013	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/cpuapr2013-1899555.html
Full Disclosure: MySQL Denial of Service Zeroday PoC	Exploit seclists.org text/html	FULLDISC 20121201 MySQL Denial of Service Zeroday PoC
Bug 882607 – CVE-2012-5614 mysql: COM_BINLOG_DUMP crash on invalid data	bugzilla.redhat.com text/html	MISC bugzilla.redhat.com/show_bug.cgi?id=882607
[MDEV-3910] COM_BINLOG_DUMP crash on invalid data - JIRA	Patch mariadb.atlassian.net text/html	MISC mariadb.atlassian.net/browse/MDEV-3910

About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 53372
oss-security - Re: Re: [Full-disclosure] MySQL (Linux) Stack based buffer overrun PoC Zeroday	www.openwall.com text/html	MLIST [oss-security] 20121202 Re: Re: [Full-disclosure] MySQL (Linux) Stack based buffer overrun PoC Zeroday
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2013:0772
Support / Security / Advisories / / MDVSA-2013:150 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:150
Gentoo Linux Documentation -- MySQL: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201308-06
MySQL Bug in UpdateXML() Lets Remote Authenticated Users Deny Service - SecurityTracker	www.securitytracker.com text/html	SECTRACK 1027829
oss-security - Re: Re: [Full-disclosure] MySQL (Linux) Stack based buffer overrun PoC Zeroday	www.openwall.com text/html	MLIST [oss-security] 20121202 Re: Re: [Full-disclosure] MySQL (Linux) Stack based buffer overrun PoC Zeroday

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mariadb	Mariadb	All	All	All	All
Application	Mariadb	Mariadb	5.5.28a	All	All	All
Application	Mariadb	Mariadb	5.5.28a	All	All	All
Application	Oracle	Mysql	5.5.19	All	All	All
Application	Oracle	Mysql	5.5.19	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	6.4	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All

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

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

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

cpe:2.3:a:oracle:mysql:5.5.19:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.5.19:*:*:*:*:*:*:*:

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

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

cpe:2.3:o:redhat:enterprise_linux_desktop:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_eus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_server_aus:6.4:*:*:*:*:*:*:*:

cpe:2.3:o:redhat:enterprise_linux_workstation:6.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→