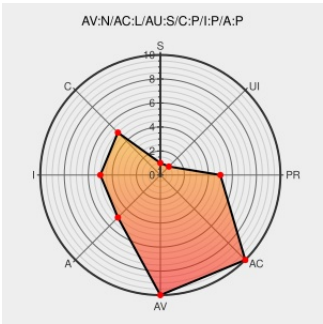
CVE-2012-5612

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

Last Modified on: 07/20/2022 04:24:00 PM UTC

CVE-2012-5612

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



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

Heap-based buffer overflow in Oracle MySQL 5.5.19 and other versions through 5.5.28, and MariaDB 5.5.28a and possibly other versions, allows remote authenticated users to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code, as demonstrated using certain variations of the (1) USE, (2) SHOW TABLES, (3) DESCRIBE, (4) SHOW FIELDS FROM, (5) SHOW COLUMNS FROM, (6) SHOW INDEX FROM, (7) CREATE TABLE, (8) DROP TABLE, (9) ALTER TABLE, (10) DELETE FROM, (11) UPDATE, and (12) SET PASSWORD commands.

CVE-2012-5612 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Full Disclosure: MySQL (Linux) Heap Based Overrun PoC Zeroday	Exploit, seclists.org, text/html	FULLDISC 20121201 MySQL (Linux) Heap Based Overrun PoC Zeroday
Repository / Oval Repository	oval.cisecurity.org, text/html	OVAL oval:org.mitre.oval:def:16960
[security-announce] SUSE-SU-2013:0262-1: important: Security update for	lists.opensuse.org, text/html	SUSE SUSE-SU-2013:0262
USN-1703-1: MySQL vulnerabilities | Ubuntu	www.ubuntu.com	UBUNTU USN-1703-1

	text/html	
Oracle Critical Patch Update - January 2013	www.oracle.com text/html	CONFIRM www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html
MySQL (Linux) Heap Based Overrun PoC Zeroday	Exploit www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 23076
About Secunia Research | Flexera	secunia.com Depreciated Link text/plain	SECUNIA 53372
Support / Security / Advisories / / MDVSA-2013:102 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:102
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
Support / Security / Advisories / / MDVSA-2013:150 | Mandriva	www.mandriva.com text/html	MANDRIVA MDVSA-2013:150
[MDEV-3908] crash in multi-table delete and mdl - JIRA	Exploit Patch mariadb.atlassian.net text/html	CONFIRM mariadb.atlassian.net/browse/MDEV-3908
Gentoo Linux Documentation -- MySQL: Multiple vulnerabilities	security.gentoo.org text/html	GENTOO GLSA-201308-06
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
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Linux	Linux	All	All	All	All
Operating System	Linux	Linux	All	All	All	All

Application	Mariadb	Mariadb	All	All	All	All
Application	Mariadb	Mariadb	10.0.0	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
Operating System	Suse	Linux Enterprise Desktop	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Server	11	sp2	All	All
Operating System	Suse	Linux Enterprise Software Development Kit	11	sp2	All	All

cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:-:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux:*:*:*:*:*:*:*:*:

cpe:2.3:o:linux:linux:*:*:*:*:*:*:*:*:

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

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

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:o:suse:linux_enterprise_desktop:11:sp2:*:*:*:*:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:-:*:*:

cpe:2.3:o:suse:linux_enterprise_server:11:sp2:*:*:*:vmware:*:*:

cpe:2.3:o:suse:linux_enterprise_software_development_kit:11:sp2:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→