



CVE-2012-5611

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

Last Modified on: 03/23/2021 11:28:20 PM UTC

CVE-2012-5611

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux](#) from [Linux](#) contain the following vulnerability:

Stack-based buffer overflow in the `acl_get` function in Oracle MySQL 5.5.19 and other versions through 5.5.28, and 5.1.53 and other versions through 5.1.66, and MariaDB 5.5.2.x before 5.5.28a, 5.3.x before 5.3.11, 5.2.x before 5.2.13 and 5.1.x before 5.1.66, allows remote authenticated users to execute arbitrary code via a long argument to the `GRANT FILE` command.

CVE-2012-5611 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) Stack based buffer overrun PoC Zeroday	seclists.org text/html	FULLDISC 20121201 MySQL (Linux) Stack based buffer overrun PoC Zeroday
[security-announce] openSUSE-SU-2013:0011-1: important: mariadb to 5.5.2	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0011
[security-announce] SUSE-SU-2013:0262-1: important: Security update for	lists.opensuse.org text/html	SUSE SUSE-SU-2013:0262
MariaDB 5.2.13 Release Notes - MariaDB Knowledge Base	kb.askmonty.org text/html	CONFIRM kb.askmonty.org/en/mariadb-5213-release-notes/
[security-announce] openSUSE-SU-2013:0013-1: important: mysql-community-	lists.opensuse.org text/html	SUSE openSUSE-SU-2013:0013
Red Hat Customer Portal	redhat.com	REDHAT RHEL 6.5-0100

Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2013:0180
USN-1703-1: MySQL vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1703-1
Oracle Critical Patch Update - January 2013	www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/cpujan2013-1515902.html
Red Hat Customer Portal	web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:1551
About Secunia Research Flexera	secunia.com Deprecated Link text/plain	 SECUNIA 53372
MySQL (Linux) Stack Based Buffer Overrun PoC Zeroday	www.exploit-db.com Proof of Concept text/html	 EXPLOIT-DB 23075
Support / Security / Advisories // MDVSA-2013:102 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2013:102
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:16395
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
Debian -- Security Information -- DSA-2581-1 mysql-5.1	www.debian.org Deprecated Link text/html	 DEBIAN DSA-2581
MariaDB 5.3.11 Release Notes - MariaDB Knowledgebase	kb.askmonty.org text/html	 CONFIRM kb.askmonty.org/en/mariadb-5311-release-notes/
Security Advisory SA51443 - MariaDB Buffer Overflow Vulnerability - Secunia	web.archive.org text/html	 SECUNIA 51443
USN-1658-1: MySQL vulnerability Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1658-1
[security-announce] openSUSE-SU-2013:0135-1: important: mysql-community-	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0135
openSUSE-SU-2013:1412-1: moderate: mariadb	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:1412
MariaDB 5.5.28a Release Notes - AskMonty KnowledgeBase	kb.askmonty.org text/html	 CONFIRM kb.askmonty.org/en/mariadb-5528a-release-notes/
Support / Security / Advisories // MDVSA-2013:150 Mandriva	www.mandriva.com text/html	 MANDRIVA MDVSA-2013:150
[security-announce] openSUSE-SU-2013:0156-1: important: mariadb to 5.1.6	lists.opensuse.org text/html	 SUSE openSUSE-SU-2013:0156
Gentoo Linux Documentation -- MySQL: Multiple vulnerabilities	security.gentoo.org text/html	 GENTOO GLSA-201308-06
MariaDB 5.1.66 Release Notes - MariaDB Knowledge Base	kb.askmonty.org text/html	 CONFIRM kb.askmonty.org/en/mariadb-5166-release-notes/
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

[security-announce] openSUSE-SU-2013:0014-1:
important: mariadb to 5.2.1

lists.opensuse.org
[text/html](#)

 SUSE openSUSE-SU-2013:0014

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Linux	Linux	All	All	All	All
Operating System	Linux	Linux	All	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	5.1.62	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	5.2.2	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	5.3.2	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	5.1.41	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	5.1.62	All	All	All
Application	Mariadb	Mariadb	5.2.0	All	All	All
Application	Mariadb	Mariadb	5.2.1	All	All	All

cpe:2.3:o:linux:linux:.*:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:o:linux:linux:.*:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.41:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.42:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.44:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.47:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.49:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.50:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.51:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.53:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.55:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.60:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.61:.*:.*:.*:.*:.*:.*:.*
cpe:2.3:a:mariadb:mariadb:5.1.62:.*:.*:.*:.*:.*:.*:.*
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:5.2.2:.*:.*:.*:.*:.*:.*:.*
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:5.3.2:*****:
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:5.1.41:*****:
cpe:2.3:a:mariadb:mariadb:5.1.42:*****:
cpe:2.3:a:mariadb:mariadb:5.1.44:*****:
cpe:2.3:a:mariadb:mariadb:5.1.47:*****:
cpe:2.3:a:mariadb:mariadb:5.1.49:*****:
cpe:2.3:a:mariadb:mariadb:5.1.50:*****:
cpe:2.3:a:mariadb:mariadb:5.1.51:*****:
cpe:2.3:a:mariadb:mariadb:5.1.53:*****:
cpe:2.3:a:mariadb:mariadb:5.1.55:*****:
cpe:2.3:a:mariadb:mariadb:5.1.60:*****:
cpe:2.3:a:mariadb:mariadb:5.1.61:*****:
cpe:2.3:a:mariadb:mariadb:5.1.62:*****:

cpe:2.3:a:mariadb:mariadb:5.1.62:::~::~~::~~::
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:5.2.2::~::~~::~~::
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:5.3.2::~::~~::~~::
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:oracle:mysql:5.1.53:*****:
cpe:2.3:a:oracle:mysql:5.5.19:*****:
cpe:2.3:a:oracle:mysql:5.1.53:*****:
cpe:2.3:a:oracle:mysql:5.5.19:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →