



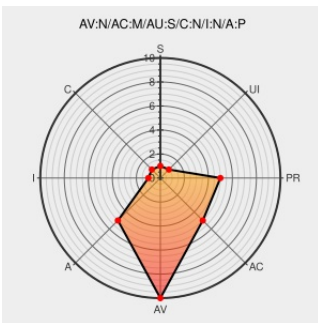
Last Modified on: 10/27/2022 03:21:00 PM UTC

CVE-2012-3167

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF 

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

Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.63 and earlier, and 5.5.25 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Full Text Search.

CVE-2012-3167 has been assigned by  secalert_us@oracle.com to track the vulnerability

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
USN-1621-1: MySQL vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-1621-1
Security Advisory SA51309 - Red Hat update for mysql - Secunia	Third Party Advisory web.archive.org text/html	 SECUNIA 51309
About Secunia Research Flexera	Third Party Advisory secunia.com Deprecated Link text/plain	 SECUNIA 53372
Security Advisory SA51177 - Ubuntu update for mysql-5.1, mysql-5.5, and mysql-dfsg-5.1 - Secunia	Third Party Advisory web.archive.org text/html	 SECUNIA 51177

IBM X-Force Exchange	Third Party Advisory VDB Entry exchange.xforce.ibmcloud.com text/html	 XF mysqlserver-serverfulltextsearch-dos(79392)
Debian -- Security Information -- DSA-2581-1 mysql-5.1	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-2581
Oracle Critical Patch Update - October 2012	Patch Vendor Advisory www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/cpuoct2012-1515893.html
Support / Security / Advisories / / MDVSA-2013:150 Mandriva	Third Party Advisory www.mandriva.com text/html	 MANDRIVA MDVSA-2013:150
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2012:1462
Gentoo Linux Documentation -- MySQL: Multiple vulnerabilities	Third Party Advisory security.gentoo.org text/html	 GENTOO GLSA-201308-06

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	Canonical	Ubuntu Linux	10.04	All	All	All
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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Canonical	Ubuntu Linux	10.04	All	All	All
Operating System	Canonical	Ubuntu Linux	11.10	All	All	All
Operating	Canonical	Ubuntu Linux	12.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	12.10	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	6.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Application	Mariadb	Mariadb	All	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	6.3	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:-:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:						
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:12.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:10.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:11.10:*:*:*:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:						
cpe:2.3:o:canonical:ubuntu_linux:12.10:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:6.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:						

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

```
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:6.3:*:*:*:*:*:*:
```

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

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

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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