



CVE-2015-4858

Published on: 10/21/2015 12:00:00 AM UTC

Last Modified on: 09/08/2022 08:43:00 PM UTC

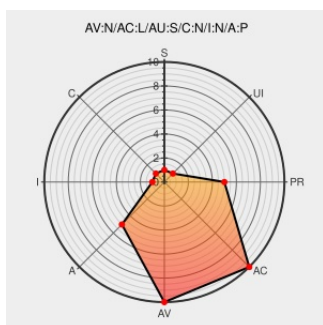
CVE-2015-4858

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2015-4913.

CVE-2015-4858 has been assigned by secalert_us@oracle.com to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

SINGLE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Oracle Solaris Bulletin - April 2016

[Vendor Advisory](#)
[www.oracle.com](#)
[text/html](#)

CONFIRM
www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html

openSUSE-SU-2016:0368-1: moderate:
Security update for mariadb

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

SUSE [openSUSE-SU-2016:0368](#)

Red Hat Customer Portal

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

REDHAT [RHSA-2016:0705](#)

Red Hat Customer Portal

[Third Party Advisory](#)
[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

REDHAT [RHSA-2016:1481](#)

	Inactive Link Not Archived	
Debian -- Security Information -- DSA-3385-1 mariadb-10.0	Third Party Advisory www.debian.org Depreciated Link text/html	 DEBIAN DSA-3385
SUSE-SU-2016:0296-1	Third Party Advisory www.suse.com text/html	 SUSE SUSE-SU-2016:0296
Oracle Critical Patch Update - October 2015	Patch Vendor Advisory www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
[SECURITY] Fedora 23 Update: mariadb-10.0.23-1.fc23	Mailing List Third Party Advisory lists.fedoraproject.org text/html	 FEDORA FEDORA-2016-e30164d0a2
Debian -- Security Information -- DSA-3377-1 mysql-5.5	Third Party Advisory www.debian.org Depreciated Link text/html	 DEBIAN DSA-3377
Oracle Linux Bulletin - April 2016	Vendor Advisory www.oracle.com text/html	 CONFIRM www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:0534
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	 REDHAT RHSA-2016:1132
Oracle MySQL Server CVE-2015-4858 Remote Security Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	 BID 77145
USN-2781-1: MySQL vulnerabilities Ubuntu	Third Party Advisory www.ubuntu.com text/html	 UBUNTU USN-2781-1
MySQL Multiple Bugs Let Remote Users Access and Modify Data, Remote and Local Users Deny Service, and Local Users Gain Elevated Privileges - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	 SECTrack 1033894
[security-announce] openSUSE-SU-2015:2246-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2246
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	 REDHAT RHSA-2016:1480
[security-announce] openSUSE-SU-2015:2244-1: important: Security update	Mailing List Third Party Advisory lists.opensuse.org text/html	 SUSE openSUSE-SU-2015:2244

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	15.10	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Fedoraproject	Fedora	23	All	All	All
Application	Mariadb	Mariadb	All	All	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Desktop	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Server	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Software Development Kit	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All
Operating System	Novell	Suse Linux Enterprise Workstation Extension	12.0	sp1	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating System	Opensuse	Leap	42.1	All	All	All
Operating	Opensuse	Opensuse	13.1	All	All	All

System						
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Oracle	Linux	7	All	All	All
Operating System	Oracle	Linux	7	-	All	All
Operating System	Oracle	Linux	7	All	All	All
Application	Oracle	Mysql	All	All	All	All
Application	Oracle	Mysql	All	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Oracle	Solaris	11.3	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.1	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.5	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Eus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node	7.0	All	All	All

Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Hpc Node Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.4	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Server Aus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	7.2	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.3	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Tus	7.7	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	7.0	All	All	All
cpe:2.3:o:canonical:ubuntu_linux:12.04:****-:****:						
cpe:2.3:o:canonical:ubuntu_linux:14.04:****.esm:****:						
cpe:2.3:o:canonical:ubuntu_linux:15.04:*****:****:						
cpe:2.3:o:canonical:ubuntu_linux:15.10:*****:****:						
cpe:2.3:o:debian:debian_linux:7.0:*****:****:						
cpe:2.3:o:debian:debian_linux:8.0:*****:****:						
cpe:2.3:o:fedoraproject:fedora:23:*****:****:						
cpe:2.3:o:openjdk:openjdk:8:*****:****:						

```
cpe:2.3:a:mariaadb:mariaadb: : : : : : : :
```

```
cpe:2.3:o:novell:suse_linux_enterprise_desktop:12.0:sp1:*:*:*:*.*
```

```
cpe:2.3:o:novell:suse_linux_enterprise_desktop:12.0:sp1:*:*:*:*:*
```

```
cpe:2.3:o:novell:suse_linux_enterprise_server:12.0:sp1:*:*:*:*:
```

```
cpe:2.3:o:novell:suse_linux_enterprise_server:12.0:sp1:*:*:*:*:
```

```
cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:12.0:sp1:*:*:*:*:
```

```
cpe:2.3:o:novell:suse_linux_enterprise_software_development_kit:12.0:sp1:*:*:*:*:
```

```
cpe:2.3:o:novell:suse_linux_enterprise_workstation_extension:12.0:sp1:*:*:*:*:
```

```
cpe:2.3:o:novell:suse_linux_enterprise_workstation_extension:12.0:sp1:*:*:*:*:
```

```
cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:leap:42.1:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:*:
```

```
cpe:2.3:o:oracle:linux:7:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:oracle:linux:7:-:*:*:*:*:*:
```

```
cpe:2.3:o:oracle:linux:7:*:*:*:*:*:*:*:
```

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

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

cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:*:

cpe:2.3:o:oracle:solaris:11.3:*:*:*:*:*:*:

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

```
cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*:
```

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

```
cpe:2.3:o:redhat:enterprise_linux:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux_eus:7.1:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_eus:7.2:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux eus:7.3:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux eus:7.4:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux eus:7.5:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux eus:7.6:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux eus:7.7:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux hpc node:7.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:hpc_node:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux:hpc_node_eus:7.2:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux hpc node eus:7.2:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux server:7.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.2:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.3.*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.4:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.6:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:redhat:enterprise linux server aus:7.7:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_server_aus:7.2:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.2:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux server eus:7.2:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.3:.*:.*:.*:.*:.*:.*:.*:.*
```

```
cpe:2.3:o:redhat:enterprise linux server tus:7.6.*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_server_tus:7.7:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise_linux_workstation:7.0:*:*:*:*:*.*
```

```
cpe:2.3:o:redhat:enterprise linux workstation:7.0:*.~*~*~*~*~*~*
```

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

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](#)