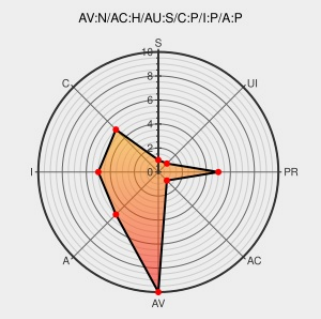
CVE-2015-4879

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

Last Modified on: 08/05/2022 02:25:00 PM UTC

CVE-2015-4879

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 5.5.44 and earlier, and 5.6.25 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to DML.

CVE-2015-4879 has been assigned by secalert_us@oracle.com to track the vulnerability

CVSS2 Score: 4.6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	HIGH	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	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
Red Hat Customer Portal	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	REDHAT RHSA-2016:1481
Debian -- Security Information -- DSA-3385-1 mariadb-10.0	Third Party Advisory, www.debian.org, Depreciated Link, text/html	DEBIAN DSA-3385
Oracle Critical Patch Update - October 2015	Patch, Vendor Advisory, www.oracle.com	CONFIRM www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html

	text/html	
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:1628
Oracle MySQL Server CVE-2015-4879 Remote Security Vulnerability	Third Party Advisory VDB Entry cve.report (archive) text/html	BID 77140
[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
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

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	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	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	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	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	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 Desktop	7.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	7.0	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	7.2	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:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:esm:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.10:*:*:*:*:*:*:*:

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

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

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:debian:debian_linux:7.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:23:*:*:*:*:*:*:*:

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

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_desktop:7.0:*:*:*:*:*:*:*:

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

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:7.2:*:*:*:*:*:*:*:

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→

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