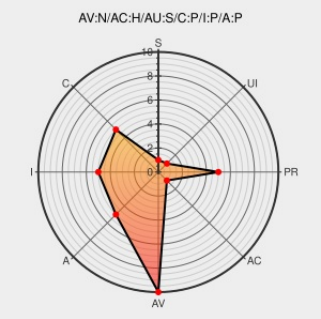
CVE-2008-4098

Published on: 09/17/2008 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:10:37 AM UTC

CVE-2008-4098

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



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

MySQL before 5.0.67 allows local users to bypass certain privilege checks by calling CREATE TABLE on a MyISAM table with modified (1) DATA DIRECTORY or (2) INDEX DIRECTORY arguments that are originally associated with pathnames without symlinks, and that can point to tables created at a future time at which a pathname is modified to contain a symlink to a subdirectory of the MySQL home data directory. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4097.

CVE-2008-4098 has been assigned by secalert@redhat.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
[security-announce] SUSE Security Summary Report: SUSE-SR:2008:025	Third Party Advisory, lists.opensuse.org, text/html	SUSE SUSE-SR:2008:025
oss-security - Re: CVE request: MySQL incomplete fix for CVE-2008-2079	Mailing List, Third Party Advisory, www.openwall.com, text/html	MLIST [oss-security] 20080909 Re: CVE request: MySQL incomplete fix for CVE-2008-2079
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Not Applicable, web.archive.org, text/html	SECUNIA 32759

oss-security - Re: CVE request: MySQL incomplete fix for CVE-2008-2079	Mailing List Third Party Advisory www.openwall.com text/html	MLIST [oss-security] 20080916 Re: CVE request: MySQL incomplete fix for CVE-2008-2079
Ubuntu update for mysql-dfsg-5 and mysql-dfsg-5.1 - Advisories - Community	Not Applicable web.archive.org text/html	SECUNIA 38517
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mysql-myisam-symlink-security-bypass(45649)
Support	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2010:0110
USN-671-1: MySQL vulnerabilities | Ubuntu	Third Party Advisory www.ubuntu.com text/html	UBUNTU USN-671-1
MySQL Bugs: #32167: another privilege bypass with DATA/INDEX DIRECTORY	Issue Tracking Patch Vendor Advisory bugs.mysql.com text/html	CONFIRM bugs.mysql.com/bug.php?id=32167
USN-897-1: MySQL vulnerabilities | Ubuntu	Third Party Advisory ubuntu.com text/html	UBUNTU USN-897-1
Security Advisory SA32578 - Debian update for mysql-dfsg-5.0 - Secunia	Not Applicable web.archive.org text/html	SECUNIA 32578
Debian -- Security Information -- DSA-1662-1 mysql-dfsg-5.0	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-1662
Support / Security / Advisories / / MDVSA-2009:094 | Mandriva	Broken Link www.mandriva.com text/html	MANDRIVA MDVSA-2009:094
#480292 - CVE-2008-2079: mysql allows local users to bypass certain privilege checks - Debian Bug report logs	Issue Tracking Third Party Advisory bugs.debian.org text/html	MISC bugs.debian.org/cgi-bin/bugreport.cgi?bug=480292#25
Repository / Oval Repository	oval.cisecurity.org text/html	OVAL oval:org.mitre.oval:def:10591
USN-1397-1: MySQL vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1397-1
Ubuntu update for mysql-dfsg-5.0 - Secunia Advisories - Vulnerability Intelligence - Secunia.com	Not Applicable web.archive.org text/html	SECUNIA 32769
Support	Third Party Advisory www.redhat.com text/html	REDHAT RHSA-2009:1067

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	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Canonical	Ubuntu Linux	6.06	All	All	All
Operating System	Canonical	Ubuntu Linux	7.10	All	All	All
Operating System	Canonical	Ubuntu Linux	8.04	All	All	All
Operating System	Canonical	Ubuntu Linux	8.10	All	All	All
Operating System	Canonical	Ubuntu Linux	9.04	All	All	All
Operating System	Canonical	Ubuntu Linux	9.10	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Operating System	Debian	Debian Linux	5.0	All	All	All
Application	Mysql	Mysql	5.0.0	All	All	All
Application	Mysql	Mysql	5.0.1	All	All	All
Application	Mysql	Mysql	5.0.10	All	All	All
Application	Mysql	Mysql	5.0.15	All	All	All
Application	Mysql	Mysql	5.0.16	All	All	All
Application	Mysql	Mysql	5.0.17	All	All	All
Application	Mysql	Mysql	5.0.2	All	All	All
Application	Mysql	Mysql	5.0.20	All	All	All
Application	Mysql	Mysql	5.0.24	All	All	All

Application	Mysql	Mysql	5.0.3	All	All	All
Application	Mysql	Mysql	5.0.30	All	All	All
Application	Mysql	Mysql	5.0.36	All	All	All
Application	Mysql	Mysql	5.0.4	All	All	All
Application	Mysql	Mysql	5.0.44	All	All	All
Application	Mysql	Mysql	5.0.5	All	All	All
Application	Mysql	Mysql	5.0.54	All	All	All
Application	Mysql	Mysql	5.0.56	All	All	All
Application	Mysql	Mysql	5.0.60	All	All	All
Application	Mysql	Mysql	5.0.66	All	All	All
Application	Mysql	Mysql	5.0.0	All	All	All
Application	Mysql	Mysql	5.0.1	All	All	All
Application	Mysql	Mysql	5.0.10	All	All	All
Application	Mysql	Mysql	5.0.15	All	All	All
Application	Mysql	Mysql	5.0.16	All	All	All
Application	Mysql	Mysql	5.0.17	All	All	All
Application	Mysql	Mysql	5.0.2	All	All	All
Application	Mysql	Mysql	5.0.20	All	All	All
Application	Mysql	Mysql	5.0.24	All	All	All
Application	Mysql	Mysql	5.0.3	All	All	All
Application	Mysql	Mysql	5.0.30	All	All	All
Application	Mysql	Mysql	5.0.36	All	All	All
Application	Mysql	Mysql	5.0.4	All	All	All
Application	Mysql	Mysql	5.0.44	All	All	All
Application	Mysql	Mysql	5.0.5	All	All	All
Application	Mysql	Mysql	5.0.54	All	All	All
Application	Mysql	Mysql	5.0.56	All	All	All
Application	Mysql	Mysql	5.0.60	All	All	All
Application	Mysql	Mysql	5.0.66	All	All	All
Application	Oracle	Mysql	5.0.23	All	All	All
Application	Oracle	Mysql	5.0.25	All	All	All
Application	Oracle	Mysql	5.0.26	All	All	All
Application	Oracle	Mysql	5.0.28	All	All	All
Application	Oracle	Mysql	5.0.30	sp1	All	All
Application	Oracle	Mysql	5.0.32	All	All	All

Application	Oracle	Mysql	5.0.34	All	All	All
Application	Oracle	Mysql	5.0.36	sp1	All	All
Application	Oracle	Mysql	5.0.38	All	All	All
Application	Oracle	Mysql	5.0.40	All	All	All
Application	Oracle	Mysql	5.0.41	All	All	All
Application	Oracle	Mysql	5.0.42	All	All	All
Application	Oracle	Mysql	5.0.44	sp1	All	All
Application	Oracle	Mysql	5.0.45	All	All	All
Application	Oracle	Mysql	5.0.46	All	All	All
Application	Oracle	Mysql	5.0.48	All	All	All
Application	Oracle	Mysql	5.0.50	All	All	All
Application	Oracle	Mysql	5.0.50	sp1	All	All
Application	Oracle	Mysql	5.0.51	All	All	All
Application	Oracle	Mysql	5.0.52	All	All	All
Application	Oracle	Mysql	5.0.56	sp1	All	All
Application	Oracle	Mysql	5.0.58	All	All	All
Application	Oracle	Mysql	5.0.60	sp1	All	All
Application	Oracle	Mysql	5.0.62	All	All	All
Application	Oracle	Mysql	5.0.64	All	All	All
Application	Oracle	Mysql	5.0.66	sp1	All	All
Application	Oracle	Mysql	5.0.23	All	All	All
Application	Oracle	Mysql	5.0.25	All	All	All
Application	Oracle	Mysql	5.0.26	All	All	All
Application	Oracle	Mysql	5.0.28	All	All	All
Application	Oracle	Mysql	5.0.30	sp1	All	All
Application	Oracle	Mysql	5.0.32	All	All	All
Application	Oracle	Mysql	5.0.34	All	All	All
Application	Oracle	Mysql	5.0.36	sp1	All	All
Application	Oracle	Mysql	5.0.38	All	All	All
Application	Oracle	Mysql	5.0.40	All	All	All
Application	Oracle	Mysql	5.0.41	All	All	All
Application	Oracle	Mysql	5.0.42	All	All	All
Application	Oracle	Mysql	5.0.44	sp1	All	All
Application	Oracle	Mysql	5.0.45	All	All	All
Application	Oracle	Mysql	5.0.46	All	All	All
Application	Oracle	Mysql	5.0.48	All	All	All

Application	Oracle	Mysql	5.0.48	All	All	All
Application	Oracle	Mysql	5.0.50	All	All	All
Application	Oracle	Mysql	5.0.50	sp1	All	All
Application	Oracle	Mysql	5.0.51	All	All	All
Application	Oracle	Mysql	5.0.52	All	All	All
Application	Oracle	Mysql	5.0.56	sp1	All	All
Application	Oracle	Mysql	5.0.58	All	All	All
Application	Oracle	Mysql	5.0.60	sp1	All	All
Application	Oracle	Mysql	5.0.62	All	All	All
Application	Oracle	Mysql	5.0.64	All	All	All
Application	Oracle	Mysql	5.0.66	sp1	All	All

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:7.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:6.06:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:7.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:8.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:9.10:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:5.0:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.16:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.17:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.20:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.24:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.30:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.36:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.44:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.54:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.56:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.60:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.66:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.0:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.16:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.17:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.20:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.24:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.30:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.36:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.44:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.54:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.56:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.60:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.66:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.23:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.25:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.26:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.28:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.30:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.32:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.34:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.36:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.38:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.40:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.41:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.42:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.44:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.45:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.46:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.48:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.50:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.50:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.51:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.52:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.56:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.58:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.60:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.62:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.64:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.66:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.23:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.25:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.26:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.28:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.30:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.32:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.34:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.36:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.38:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.40:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.41:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.42:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.44:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.45:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.46:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.48:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.50:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.50:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.51:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.52:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.56:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.58:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.60:sp1:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.62:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.64:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.66:sp1:*:*:*:*:*:*: