

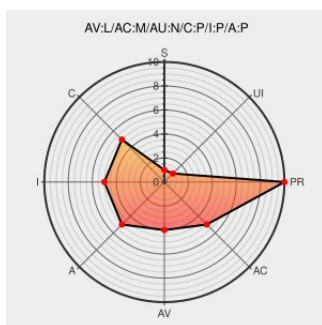


CVE-2009-4030

Published on: 11/30/2009 12:00:00 AM UTC

Last Modified on: 02/13/2023 02:20:00 AM UTC

CVE-2009-4030

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

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

MySQL 5.1.x before 5.1.41 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 data home directory, related to incorrect calculation of the mysql_unpacked_real_data_home value. NOTE: this vulnerability exists because of an incomplete fix for CVE-2008-4098 and CVE-2008-2079.

CVE-2009-4030 has been assigned by [secalert@redhat.com](#) to track the vulnerability

CVSS2 Score: **4.4 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

MEDIUM

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

[security-announce] SUSE Security Summary Report: SUSE-SR:2010:021

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

[SUSE SUSE-SR:2010:021](#)

MySQL Lists: commits: bzd commit into mysql-5.0-bugteam branch (joro:2845) Bug#32167

[lists.mysql.com](#)
[text/html](#)

[MLIST \[commits\] 20091110 bzd commit into mysql-5.0-bugteam branch \(joro:2845\) Bug#32167](#)

Ubuntu update for mysql-dfsg-5 and mysql-dfsg-5.1 - Advisories - Community

[web.archive.org](#)
[text/html](#)

[SECUNIA 38517](#)

Support

[www.redhat.com](#)

[RFDHAT RHSA-2010:0110](#)

Support	www.redhat.com text/html	 REDHAT RHSA-2010:0109
oss-security - mysql-5.1.41	www.openwall.com text/html	 MLIST [oss-security] 20091119 mysql-5.1.41
MySQL Bugs: #32167: another privilege bypass with DATA/INDEX DIRECTORY	bugs.mysql.com text/html	 CONFIRM bugs.mysql.com/bug.php?id=32167
'Re: [oss-security] mysql-5.1.41' - MARC	marc.info text/html	 MLIST [oss-security] 20091124 Re: mysql-5.1.41
USN-897-1: MySQL vulnerabilities Ubuntu	ubuntu.com text/html	 UBUNTU USN-897-1
Debian -- Security Information -- DSA-1997-1 mysql-dfsg-5.0	www.debian.org Deprecated Link text/html	 DEBIAN DSA-1997
APPLE-SA-2010-03-29-1 Security Update 2010-002 / Mac OS X v10.6.3	lists.apple.com text/html	 APPLE APPLE-SA-2010-03-29-1
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:011	lists.opensuse.org text/html	 SUSE SUSE-SR:2010:011
Debian update for mysql-dfsg-5.0 - Secunia.com	web.archive.org text/html	 SECUNIA 38573
'Re: [oss-security] mysql-5.1.41' - MARC	marc.info text/html	 MLIST [oss-security] 20091124 Re: mysql-5.1.41
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:11116
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval.org.mitre.oval:def:8156
USN-1397-1: MySQL vulnerabilities Ubuntu	www.ubuntu.com text/html	 UBUNTU USN-1397-1
oss-security - Re: mysql-5.1.41	www.openwall.com text/html	 MLIST [oss-security] 20091124 Re: mysql-5.1.41
Support	www.redhat.com text/html	 REDHAT RHSA-2010:0109
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	 VUPEN ADV-2010-1107
About the security content of Security Update 2010-002 / Mac OS X v10.6.3	support.apple.com text/html	 CONFIRM support.apple.com/kb/HT4077
MySQL :: MySQL 5.1 Reference Manual :: C.1.2 Changes in MySQL 5.1.41 (05 November 2009)	web.archive.org text/html Inactive Link Not Archived	 CONFIRM dev.mysql.com/doc/refman/5.1/en/news-5-1-41.html

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
Application	Mysql	Mysql	5.1.23	All	All	All
Application	Mysql	Mysql	5.1.32	All	All	All
Application	Mysql	Mysql	5.1.5	All	All	All
Application	Mysql	Mysql	5.1.23	All	All	All
Application	Mysql	Mysql	5.1.32	All	All	All
Application	Mysql	Mysql	5.1.5	All	All	All
Application	Oracle	Mysql	5.1	All	All	All
Application	Oracle	Mysql	5.1.1	All	All	All
Application	Oracle	Mysql	5.1.10	All	All	All
Application	Oracle	Mysql	5.1.11	All	All	All
Application	Oracle	Mysql	5.1.12	All	All	All
Application	Oracle	Mysql	5.1.13	All	All	All
Application	Oracle	Mysql	5.1.14	All	All	All
Application	Oracle	Mysql	5.1.15	All	All	All
Application	Oracle	Mysql	5.1.16	All	All	All
Application	Oracle	Mysql	5.1.17	All	All	All
Application	Oracle	Mysql	5.1.18	All	All	All
Application	Oracle	Mysql	5.1.19	All	All	All
Application	Oracle	Mysql	5.1.2	All	All	All
Application	Oracle	Mysql	5.1.20	All	All	All
Application	Oracle	Mysql	5.1.21	All	All	All
Application	Oracle	Mysql	5.1.22	All	All	All
Application	Oracle	Mysql	5.1.3	All	All	All
Application	Oracle	Mysql	5.1.30	All	All	All
Application	Oracle	Mysql	5.1.4	All	All	All
Application	Oracle	Mysql	5.1.6	All	All	All
Application	Oracle	Mysql	5.1.7	All	All	All
Application	Oracle	Mysql	5.1.8	All	All	All
Application	Oracle	Mysql	5.1.9	All	All	All
Application	Oracle	Mysql	5.1	All	All	All
Application	Oracle	Mysql	5.1.1	All	All	All
Application	Oracle	Mysql	5.1.10	All	All	All
Application	Oracle	Mysql	5.1.11	All	All	All
Application	Oracle	Mysql	5.1.12	All	All	All
Application	Oracle	Mysql	5.1.13	All	All	All

Application	Oracle	Mysql	5.1.14	All	All	All
Application	Oracle	Mysql	5.1.15	All	All	All
Application	Oracle	Mysql	5.1.16	All	All	All
Application	Oracle	Mysql	5.1.17	All	All	All
Application	Oracle	Mysql	5.1.18	All	All	All
Application	Oracle	Mysql	5.1.19	All	All	All
Application	Oracle	Mysql	5.1.2	All	All	All
Application	Oracle	Mysql	5.1.20	All	All	All
Application	Oracle	Mysql	5.1.21	All	All	All
Application	Oracle	Mysql	5.1.22	All	All	All
Application	Oracle	Mysql	5.1.3	All	All	All
Application	Oracle	Mysql	5.1.30	All	All	All
Application	Oracle	Mysql	5.1.4	All	All	All
Application	Oracle	Mysql	5.1.6	All	All	All
Application	Oracle	Mysql	5.1.7	All	All	All
Application	Oracle	Mysql	5.1.8	All	All	All
Application	Oracle	Mysql	5.1.9	All	All	All
cpe:2.3:a:mysql:mysql:5.1.23:*****:						
cpe:2.3:a:mysql:mysql:5.1.32:*****:						
cpe:2.3:a:mysql:mysql:5.1.5:*****:						
cpe:2.3:a:mysql:mysql:5.1.23:*****:						
cpe:2.3:a:mysql:mysql:5.1.32:*****:						
cpe:2.3:a:mysql:mysql:5.1.5:*****:						
cpe:2.3:a:oracle:mysql:5.1:*****:						
cpe:2.3:a:oracle:mysql:5.1.1:*****:						
cpe:2.3:a:oracle:mysql:5.1.10:*****:						
cpe:2.3:a:oracle:mysql:5.1.11:*****:						
cpe:2.3:a:oracle:mysql:5.1.12:*****:						
cpe:2.3:a:oracle:mysql:5.1.13:*****:						
cpe:2.3:a:oracle:mysql:5.1.14:*****:						
cpe:2.3:a:oracle:mysql:5.1.15:*****:						
cpe:2.3:a:oracle:mysql:5.1.16:*****:						

cpe:2.3:a:oracle:mysql:5.1.16:*****:
cpe:2.3:a:oracle:mysql:5.1.17:*****:
cpe:2.3:a:oracle:mysql:5.1.18:*****:
cpe:2.3:a:oracle:mysql:5.1.19:*****:
cpe:2.3:a:oracle:mysql:5.1.2:*****:
cpe:2.3:a:oracle:mysql:5.1.20:*****:
cpe:2.3:a:oracle:mysql:5.1.21:*****:
cpe:2.3:a:oracle:mysql:5.1.22:*****:
cpe:2.3:a:oracle:mysql:5.1.3:*****:
cpe:2.3:a:oracle:mysql:5.1.30:*****:
cpe:2.3:a:oracle:mysql:5.1.4:*****:
cpe:2.3:a:oracle:mysql:5.1.6:*****:
cpe:2.3:a:oracle:mysql:5.1.7:*****:
cpe:2.3:a:oracle:mysql:5.1.8:*****:
cpe:2.3:a:oracle:mysql:5.1.9:*****:
cpe:2.3:a:oracle:mysql:5.1:*****:
cpe:2.3:a:oracle:mysql:5.1.1:*****:
cpe:2.3:a:oracle:mysql:5.1.10:*****:
cpe:2.3:a:oracle:mysql:5.1.11:*****:
cpe:2.3:a:oracle:mysql:5.1.12:*****:
cpe:2.3:a:oracle:mysql:5.1.13:*****:
cpe:2.3:a:oracle:mysql:5.1.14:*****:
cpe:2.3:a:oracle:mysql:5.1.15:*****:
cpe:2.3:a:oracle:mysql:5.1.16:*****:
cpe:2.3:a:oracle:mysql:5.1.17:*****:
cpe:2.3:a:oracle:mysql:5.1.18:*****:
cpe:2.3:a:oracle:mysql:5.1.19:*****:
cpe:2.3:a:oracle:mysql:5.1.2:*****:
cpe:2.3:a:oracle:mysql:5.1.20:*****:

cpe:2.3:a:oracle:mysql:5.1.21:*****:
cpe:2.3:a:oracle:mysql:5.1.22:*****:
cpe:2.3:a:oracle:mysql:5.1.3:*****:
cpe:2.3:a:oracle:mysql:5.1.30:*****:
cpe:2.3:a:oracle:mysql:5.1.4:*****:
cpe:2.3:a:oracle:mysql:5.1.6:*****:
cpe:2.3:a:oracle:mysql:5.1.7:*****:
cpe:2.3:a:oracle:mysql:5.1.8:*****:
cpe:2.3:a:oracle:mysql:5.1.9:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)