



CVE-2004-0388

Published on: 04/16/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:12 PM UTC

CVE-2004-0388

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

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

The `mysqld_multi` script in MySQL allows local users to overwrite arbitrary files via a symlink attack.

CVE-2004-0388 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

PARTIAL

Availability
Impact

NONE

CVE References

Description

Tags

Link

Repository / Oval Repository

[oval.cisecurity.org](#)
[text/html](#)

OVAL [oval:org.mitre.oval:def:10559](#)

'[OpenPKG-SA-2004.014] OpenPKG Security Advisory (mysql)' - MARC

[marc.info](#)
[text/html](#)

BUGTRAQ 20040414 [OpenPKG-SA-2004.014] OpenPKG Security Advisory (mysql)

redhat.com | Red Hat Support

[www.redhat.com](#)
[text/html](#)

REDHAT RHSA-2004:597

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

XF mysql-mysqldmulti-symlink(15883)

Secunia - Advisories - MySQL "mysqlbug" Insecure Temporary File Creation Vulnerability

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

SECUNIA 11223

SecurityTracker.com Archives - MySQL 'mysqld_multi'

[securitytracker.com](#)

SECTRAK 1009784

Temporary File Flaw Lets Local Users Overwrite Files	text/html	
Debian -- Security Information -- DSA-483-1 mysql	Patch Vendor Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-483
MySQL Reference Manual for version 5.0.3-alpha :: D.2.9 Changes in release 4.1.2 (28 May 2004)	web.archive.org text/html Inactive Link Not Archived	 CONFIRM dev.mysql.com/doc/mysql/en/news-4-1-2.html
Advisories - Mandriva	www.mandriva.com text/html	 MANDRAKE MDKSA-2004:034
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 6421
Gentoo Linux Documentation -- Insecure Temporary File Creation In MySQL	Vendor Advisory security.gentoo.org text/html	 GENTOO GLSA-200405-20
P-018: Red Hat Update MySQL Packages Fix Security Issues and Bugs	web.archive.org text/html Inactive Link Not Archived	 CIAC P-018
redhat.com Red Hat Support	www.redhat.com text/html	 REDHAT RHSA-2004:569
MySQL MYSQLD_Multi Insecure Temporary File Creation Vulnerability	cve.report (archive) text/html	 BID 10142

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	Oracle	Mysql	5.0.33	All	All	All
Application	Oracle	Mysql	5.0.33	All	All	All
cpe:2.3:a:oracle:mysql:5.0.33:*****:*						
cpe:2.3:a:oracle:mysql:5.0.33:*****:*						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)