



CVE-2003-1331

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:43 PM UTC

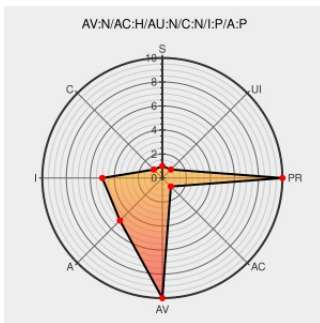
CVE-2003-1331

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



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

Stack-based buffer overflow in the `mysql_real_connect` function in the MySQL client library (`libmysqlclient`) 4.0.13 and earlier allows local users to execute arbitrary code via a long socket name, a different vulnerability than CVE-2001-1453.

CVE-2003-1331 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

HIGH

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

MySQL libmysqlclient Library `mysql_real_connect()`
Buffer Overrun Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID 7887](#)

IBM X-Force Exchange

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

[XF mysql-mysqrealconnect-bo\(12337\)](#)

NEOHAPSIS - Peace of Mind Through Integrity and
Insight

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

[FULLDISC 20030612 libmysqlclient 4.x and
below mysql_real_connect\(\) buffer overflow.](#)

MySQL Bugs: #564: `mysql_real_connect` buffer
overflow in unix socket name.

[Exploit](#)
[bugs.mysql.com](#)
[text/html](#)

[CONFIRM bugs.mysql.com/bug.php?id=564](#)

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,

are more appropriate for your purposes. CVEreport does not necessarily endorse the views expressed, or content that are made accessible on these sites. 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	All	gamma	All	All
cpe:2.3:a:oracle:mysql:*:gamma:*:*:*:*:						

← Previous ID

Next ID→