



CVE-2005-2558

Published on: 08/16/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:27 PM UTC

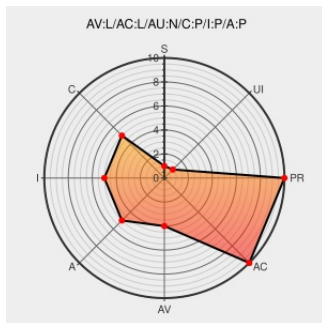
CVE-2005-2558

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



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

Stack-based buffer overflow in the init_syms function in MySQL 4.0 before 4.0.25, 4.1 before 4.1.13, and 5.0 before 5.0.7-beta allows remote authenticated users who can create user-defined functions to execute arbitrary code via a long function_name field.

CVE-2005-2558 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

IBM X-Force Exchange

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

[XF mysql-user-defined-function-bo\(21737\)](#)

[ftp.sco.com](#)
[text/plain](#)

[SCO SCOSA-2006.18](#)

Sun Solaris MySQL Multiple Vulnerabilities - Advisories - Secunia

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

[SECUNIA 29847](#)

Security Announcement

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

[SUSE SUSE-SR:2005:021](#)

usn/usn-180-1 - Ubuntu Linux

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

[UBUNTU USN-180-1](#)

No Description Provided

[sunsolve.sun.com](#)

[SUNALERT 236703](#)

Inactive Link Not Archived

MySQL User-Defined Function Buffer Overflow Vulnerability

Patch
cve.report (archive)
text/html

BID 14509

Debian -- Security Information -- DSA-833-2 mysql-dfsg-4.1

www.debian.org
Deprecated Link
text/html

DEBIAN DSA-833

[Full-disclosure] [AppSecInc Advisory MYSQL05-V0002] Buffer Overflow in MySQL User Defined Functions

Patch
Vendor Advisory
web.archive.org
text/html
Inactive Link Not Archived

FULLDISC 20050808 [AppSecInc Advisory MYSQL05-V0002] Buffer Overflow in MySQL User Defined Functions

[FLSA-2006:167803] Updated mysql packages fix security issues

www.redhat.com
text/html

FEDORA FLSA-2006:167803

Debian -- Security Information -- DSA-831-1 mysql-dfsg

www.debian.org
Deprecated Link
text/html

DEBIAN DSA-831

'[AppSecInc Advisory MYSQL05-V0002] Buffer Overflow in MySQL User' - MARC

marc.info
text/html

BUGTRAQ 20050808 [AppSecInc Advisory MYSQL05-V0002] Buffer Overflow in MySQL User Defined Functions

Advisories - Mandriva

www.mandriva.com
text/html

MANDRIVA MDKSA-2005:163

usn/usn-180-2 - Ubuntu Linux

www.ubuntu.com
text/html

UBUNTU USN-180-2

Debian -- Security Information -- DSA-829-1 mysql

www.debian.org
Deprecated Link
text/html

DEBIAN DSA-829

Secunia - Advisories - SUSE Updates for Multiple Packages

web.archive.org
text/html

SECUNIA 17027

Secunia - Advisories - UnixWare update for MySQL

web.archive.org
text/html

SECUNIA 20381

Application Security Inc. - Securing Business by Securing Enterprise Applications

Patch
Vendor Advisory
www.appsecinc.com
text/html

MISC
www.appsecinc.com/resources/alerts/mysql/2005-002.html

Webmail - OVH

www.vupen.com
text/html

VUPEN ADV-2008-1326

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	4.1.0	All	All	All

Application	Mysql	Mysql	4.1.10	All	All	All
Application	Mysql	Mysql	4.1.3	All	All	All
Application	Mysql	Mysql	5.0.1	All	All	All
Application	Mysql	Mysql	5.0.2	All	All	All
Application	Mysql	Mysql	5.0.3	All	All	All
Application	Mysql	Mysql	5.0.4	All	All	All
Application	Mysql	Mysql	4.1.0	All	All	All
Application	Mysql	Mysql	4.1.10	All	All	All
Application	Mysql	Mysql	4.1.3	All	All	All
Application	Mysql	Mysql	5.0.1	All	All	All
Application	Mysql	Mysql	5.0.2	All	All	All
Application	Mysql	Mysql	5.0.3	All	All	All
Application	Mysql	Mysql	5.0.4	All	All	All
Application	Oracle	Mysql	4.0.0	All	All	All
Application	Oracle	Mysql	4.0.1	All	All	All
Application	Oracle	Mysql	4.0.10	All	All	All
Application	Oracle	Mysql	4.0.11	All	All	All
Application	Oracle	Mysql	4.0.11	gamma	All	All
Application	Oracle	Mysql	4.0.12	All	All	All
Application	Oracle	Mysql	4.0.13	All	All	All
Application	Oracle	Mysql	4.0.14	All	All	All
Application	Oracle	Mysql	4.0.15	All	All	All
Application	Oracle	Mysql	4.0.18	All	All	All
Application	Oracle	Mysql	4.0.2	All	All	All
Application	Oracle	Mysql	4.0.20	All	All	All
Application	Oracle	Mysql	4.0.21	All	All	All
Application	Oracle	Mysql	4.0.24	All	All	All
Application	Oracle	Mysql	4.0.3	All	All	All
Application	Oracle	Mysql	4.0.4	All	All	All
Application	Oracle	Mysql	4.0.5	All	All	All
Application	Oracle	Mysql	4.0.5a	All	All	All
Application	Oracle	Mysql	4.0.6	All	All	All
Application	Oracle	Mysql	4.0.7	All	All	All
Application	Oracle	Mysql	4.0.7	gamma	All	All
Application	Oracle	Mysql	4.0.8	All	All	All

Application	Oracle	Mysql	4.0.8	gamma	All	All
Application	Oracle	Mysql	4.0.9	All	All	All
Application	Oracle	Mysql	4.0.9	gamma	All	All
Application	Oracle	Mysql	4.1.0	alpha	All	All
Application	Oracle	Mysql	4.1.2	alpha	All	All
Application	Oracle	Mysql	4.1.3	beta	All	All
Application	Oracle	Mysql	4.1.4	All	All	All
Application	Oracle	Mysql	4.1.5	All	All	All
Application	Oracle	Mysql	5.0.0	alpha	All	All
Application	Oracle	Mysql	4.0.0	All	All	All
Application	Oracle	Mysql	4.0.1	All	All	All
Application	Oracle	Mysql	4.0.10	All	All	All
Application	Oracle	Mysql	4.0.11	All	All	All
Application	Oracle	Mysql	4.0.11	gamma	All	All
Application	Oracle	Mysql	4.0.12	All	All	All
Application	Oracle	Mysql	4.0.13	All	All	All
Application	Oracle	Mysql	4.0.14	All	All	All
Application	Oracle	Mysql	4.0.15	All	All	All
Application	Oracle	Mysql	4.0.18	All	All	All
Application	Oracle	Mysql	4.0.2	All	All	All
Application	Oracle	Mysql	4.0.20	All	All	All
Application	Oracle	Mysql	4.0.21	All	All	All
Application	Oracle	Mysql	4.0.24	All	All	All
Application	Oracle	Mysql	4.0.3	All	All	All
Application	Oracle	Mysql	4.0.4	All	All	All
Application	Oracle	Mysql	4.0.5	All	All	All
Application	Oracle	Mysql	4.0.5a	All	All	All
Application	Oracle	Mysql	4.0.6	All	All	All
Application	Oracle	Mysql	4.0.7	All	All	All
Application	Oracle	Mysql	4.0.7	gamma	All	All
Application	Oracle	Mysql	4.0.8	All	All	All
Application	Oracle	Mysql	4.0.8	gamma	All	All
Application	Oracle	Mysql	4.0.9	All	All	All
Application	Oracle	Mysql	4.0.9	gamma	All	All
Application	Oracle	Mysql	4.1.0	alpha	All	All
Application	Oracle	Mysql	4.1.0	alpha	All	All

Application	Oracle	Mysql	4.1.2	alpha	All	All
Application	Oracle	Mysql	4.1.3	beta	All	All
Application	Oracle	Mysql	4.1.4	All	All	All
Application	Oracle	Mysql	4.1.5	All	All	All
Application	Oracle	Mysql	5.0.0	alpha	All	All
cpe:2.3:a:mysql:mysql:4.1.0:*****:						
cpe:2.3:a:mysql:mysql:4.1.10:*****:						
cpe:2.3:a:mysql:mysql:4.1.3:*****:						
cpe:2.3:a:mysql:mysql:5.0.1:*****:						
cpe:2.3:a:mysql:mysql:5.0.2:*****:						
cpe:2.3:a:mysql:mysql:5.0.3:*****:						
cpe:2.3:a:mysql:mysql:5.0.4:*****:						
cpe:2.3:a:mysql:mysql:4.1.0:*****:						
cpe:2.3:a:mysql:mysql:4.1.10:*****:						
cpe:2.3:a:mysql:mysql:4.1.3:*****:						
cpe:2.3:a:mysql:mysql:5.0.1:*****:						
cpe:2.3:a:mysql:mysql:5.0.2:*****:						
cpe:2.3:a:mysql:mysql:5.0.3:*****:						
cpe:2.3:a:mysql:mysql:5.0.4:*****:						
cpe:2.3:a:oracle:mysql:4.0.0:*****:						
cpe:2.3:a:oracle:mysql:4.0.1:*****:						
cpe:2.3:a:oracle:mysql:4.0.10:*****:						
cpe:2.3:a:oracle:mysql:4.0.11:*****:						
cpe:2.3:a:oracle:mysql:4.0.11:gamma:*****:						
cpe:2.3:a:oracle:mysql:4.0.12:*****:						
cpe:2.3:a:oracle:mysql:4.0.13:*****:						
cpe:2.3:a:oracle:mysql:4.0.14:*****:						
cpe:2.3:a:oracle:mysql:4.0.15:*****:						
cpe:2.3:a:oracle:mysql:4.0.18:*****:						
cpe:2.3:a:oracle:mysql:4.0.2:*****:						

cpe:2.3:a:oracle:mysql:4.0.20:*****:
cpe:2.3:a:oracle:mysql:4.0.21:*****:
cpe:2.3:a:oracle:mysql:4.0.24:*****:
cpe:2.3:a:oracle:mysql:4.0.3:*****:
cpe:2.3:a:oracle:mysql:4.0.4:*****:
cpe:2.3:a:oracle:mysql:4.0.5:*****:
cpe:2.3:a:oracle:mysql:4.0.5a:*****:
cpe:2.3:a:oracle:mysql:4.0.6:*****:
cpe:2.3:a:oracle:mysql:4.0.7:*****:
cpe:2.3:a:oracle:mysql:4.0.7:gamma:*****:
cpe:2.3:a:oracle:mysql:4.0.8:*****:
cpe:2.3:a:oracle:mysql:4.0.8:gamma:*****:
cpe:2.3:a:oracle:mysql:4.0.9:*****:
cpe:2.3:a:oracle:mysql:4.0.9:gamma:*****:
cpe:2.3:a:oracle:mysql:4.1.0:alpha:*****:
cpe:2.3:a:oracle:mysql:4.1.2:alpha:*****:
cpe:2.3:a:oracle:mysql:4.1.3:beta:*****:
cpe:2.3:a:oracle:mysql:4.1.4:*****:
cpe:2.3:a:oracle:mysql:4.1.5:*****:
cpe:2.3:a:oracle:mysql:5.0.0:alpha:*****:
cpe:2.3:a:oracle:mysql:4.0.0:*****:
cpe:2.3:a:oracle:mysql:4.0.1:*****:
cpe:2.3:a:oracle:mysql:4.0.10:*****:
cpe:2.3:a:oracle:mysql:4.0.11:*****:
cpe:2.3:a:oracle:mysql:4.0.11:gamma:*****:
cpe:2.3:a:oracle:mysql:4.0.12:*****:
cpe:2.3:a:oracle:mysql:4.0.13:*****:
cpe:2.3:a:oracle:mysql:4.0.14:*****:

cpe:2.3:a:oracle:mysql:4.0.15:*****:
cpe:2.3:a:oracle:mysql:4.0.18:*****:
cpe:2.3:a:oracle:mysql:4.0.2:*****:
cpe:2.3:a:oracle:mysql:4.0.20:*****:
cpe:2.3:a:oracle:mysql:4.0.21:*****:
cpe:2.3:a:oracle:mysql:4.0.24:*****:
cpe:2.3:a:oracle:mysql:4.0.3:*****:
cpe:2.3:a:oracle:mysql:4.0.4:*****:
cpe:2.3:a:oracle:mysql:4.0.5:*****:
cpe:2.3:a:oracle:mysql:4.0.5a:*****:
cpe:2.3:a:oracle:mysql:4.0.6:*****:
cpe:2.3:a:oracle:mysql:4.0.7:*****:
cpe:2.3:a:oracle:mysql:4.0.7:gamma:*****:
cpe:2.3:a:oracle:mysql:4.0.8:*****:
cpe:2.3:a:oracle:mysql:4.0.8:gamma:*****:
cpe:2.3:a:oracle:mysql:4.0.9:*****:
cpe:2.3:a:oracle:mysql:4.0.9:gamma:*****:
cpe:2.3:a:oracle:mysql:4.1.0:alpha:*****:
cpe:2.3:a:oracle:mysql:4.1.2:alpha:*****:
cpe:2.3:a:oracle:mysql:4.1.3:beta:*****:
cpe:2.3:a:oracle:mysql:4.1.4:*****:
cpe:2.3:a:oracle:mysql:4.1.5:*****:
cpe:2.3:a:oracle:mysql:5.0.0:alpha:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

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](#)