

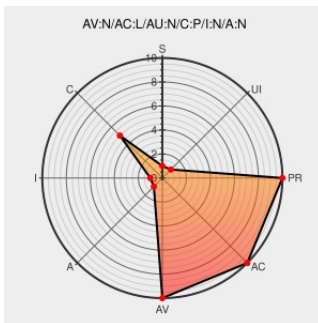


CVE-2005-2573

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

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2573

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

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

The `mysql_create_function` function in `sql_udf.cc` for MySQL 4.0 before 4.0.25, 4.1 before 4.1.13, and 5.0 before 5.0.7-beta, when running on Windows, uses an incomplete blacklist in a directory traversal check, which allows attackers to include arbitrary files via the backslash (`\`) character.

CVE-2005-2573 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

'[AppSecInc Advisory MYSQL05-V0001] Improper Filtering of Directory' - MARC

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

[BUGTRAQ 20050808 \[AppSecInc Advisory MYSQL05-V0001\] Improper Filtering of Directory Traversal Characters in MySQL User Defined Functions](#)

[Full-disclosure] [AppSecInc Advisory MYSQL05-V0001] Improper Filtering of Directory Traversal Characters in MySQL User Defined Functions

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

[FULLDISC 20050808 \[AppSecInc Advisory MYSQL05-V0001\] Improper Filtering of Directory Traversal Characters in MySQL User Defined Functions](#)

No Description Provided

[mysql.bkbits.net](#)

[Inactive Link](#) [Not Archived](#)

[CONFIRM mysql.bkbits.net:8080/mysql-4.0/cset@428b981bg2iwh3CbGANDaF-W6DbttA](#)

IBM X-Force Exchange

exchange.xforce.ibmcloud.com
text/html

 XF mysql-udf-directory-traversal(21738)

No Description Provided

mysql.bkbits.net

Inactive Link Not Archived

 CONFIRM mysql.bkbits.net:8080/mysql-4.0/gnupatch@428b981bg2iwh3CbGANDaF-W6DbttA

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	4.1.2	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.4.1.5.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→](#)