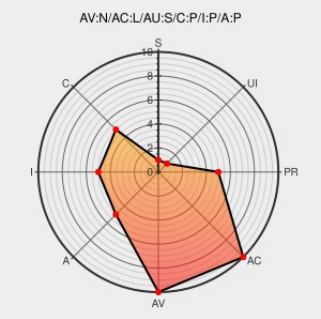
CVE-2006-1518

Published on: 05/05/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:00 PM UTC

CVE-2006-1518

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Mysql from Mysql contain the following vulnerability:

Buffer overflow in the open_table function in sql_base.cc in MySQL 5.0.x up to 5.0.20 might allow remote attackers to execute arbitrary code via crafted COM_TABLE_DUMP packets with invalid length values.

CVE-2006-1518 has been assigned by security@debian.org to track the vulnerability

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
SecurityReason - MySQL COM_TABLE_DUMP Information Leakage and Arbitrary commandexecution.	securityreason.com text/html	SREASON 839
Wisec - The WIse SECurity	Patch www.wisec.it text/html	MISC www.wisec.it/vulns.php?page=8
MySQL Remote Information Disclosure and Buffer Overflow Vulnerabilities	cve.report (archive) text/html	BID 17780
SUSE update for mysql - Advisories - Secunia	web.archive.org text/html	SECUNIA 20762
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20060502 MySQL COM_TABLE_DUMP Information Leakage and Arbitrary commandexecution.

SUSE Updates for Multiple Packages - Advisories - Secunia	web.archive.org text/html	SECUNIA 20457
Security Announcement	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SR:2006:012
MySQL AB :: MySQL 5.0 Reference Manual :: G.1.8 Changes in release 5.0.21 (02 May 2006)	Patch web.archive.org text/html Inactive Link Not Archived	CONFIRM dev.mysql.com/doc/refman/5.0/en/news-5-0-21.html
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF mysql-comtabledump-bo(26232)
Webmail : Solution de messagerie professionnelle - OVHcloud-OVH	www.vupen.com text/html	VUPEN ADV-2006-1633
Debian -- Security Information -- DSA-1079-1 mysql-dfsg	www.debian.org Depreciated Link text/html	DEBIAN DSA-1079
Debian update for mysql-dfsg - Advisories - Secunia	web.archive.org text/html	SECUNIA 20241
SuSE Security announcements: [suse-security-announce] SUSE Security Announcement: mysql remote code execution (SUSE-SA:2006:036)	web.archive.org text/html Inactive Link Not Archived	SUSE SUSE-SA:2006:036
US-CERT Vulnerability Note VU#602457	Patch Third Party Advisory US Government Resource www.kb.cert.org text/html	CERT-VN VU#602457
MySQL Information Disclosure and Buffer Overflow Vulnerabilities - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19929
Debian update for mysql-dfsg - Advisories - Secunia	web.archive.org text/html	SECUNIA 20333
Debian -- Security Information -- DSA-1071-1 mysql	www.debian.org Depreciated Link text/html	DEBIAN DSA-1071
Debian -- Security Information -- DSA-1073-1 mysql-dfsg-4.1	www.debian.org Depreciated Link text/html	DEBIAN DSA-1073
#365939 - SECURITY: MySQL COM_TABLE_DUMP Information Leakage and Arbitrary command execution - Debian Bug report logs	Patch bugs.debian.org text/html	CONFIRM bugs.debian.org/cgi-bin/bugreport.cgi?bug=365939
Debian update for mysql - Advisories - Secunia	web.archive.org text/html	SECUNIA 20253
SecurityTracker.com Archives - MySQL COM_TABLE_DUMP Processing Lets Remote Authenticated Users Execute Arbitrary Code or Obtain Information	Patch securitytracker.com text/html	SECTRACK 1016016

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	5.0.1	All	All	All
Application	Mysql	Mysql	5.0.10	All	All	All
Application	Mysql	Mysql	5.0.15	All	All	All
Application	Mysql	Mysql	5.0.16	All	All	All
Application	Mysql	Mysql	5.0.17	All	All	All
Application	Mysql	Mysql	5.0.2	All	All	All
Application	Mysql	Mysql	5.0.20	All	All	All
Application	Mysql	Mysql	5.0.3	All	All	All
Application	Mysql	Mysql	5.0.4	All	All	All
Application	Mysql	Mysql	5.0.5	All	All	All
Application	Mysql	Mysql	5.0.1	All	All	All
Application	Mysql	Mysql	5.0.10	All	All	All
Application	Mysql	Mysql	5.0.15	All	All	All
Application	Mysql	Mysql	5.0.16	All	All	All
Application	Mysql	Mysql	5.0.17	All	All	All
Application	Mysql	Mysql	5.0.2	All	All	All
Application	Mysql	Mysql	5.0.20	All	All	All
Application	Mysql	Mysql	5.0.3	All	All	All
Application	Mysql	Mysql	5.0.4	All	All	All
Application	Mysql	Mysql	5.0.5	All	All	All
Application	Oracle	Mysql	5.0.0	alpha	All	All
Application	Oracle	Mysql	5.0.11	All	All	All
Application	Oracle	Mysql	5.0.12	All	All	All
Application	Oracle	Mysql	5.0.13	All	All	All
Application	Oracle	Mysql	5.0.14	All	All	All
Application	Oracle	Mysql	5.0.18	All	All	All
Application	Oracle	Mysql	5.0.19	All	All	All
Application	Oracle	Mysql	5.0.3	beta	All	All
Application	Oracle	Mysql	5.0.6	All	All	All
Application	Oracle	Mysql	5.0.7	All	All	All

Application	Oracle	Mysql	5.0.8	All	All	All
Application	Oracle	Mysql	5.0.9	All	All	All
Application	Oracle	Mysql	5.0.0	alpha	All	All
Application	Oracle	Mysql	5.0.11	All	All	All
Application	Oracle	Mysql	5.0.12	All	All	All
Application	Oracle	Mysql	5.0.13	All	All	All
Application	Oracle	Mysql	5.0.14	All	All	All
Application	Oracle	Mysql	5.0.18	All	All	All
Application	Oracle	Mysql	5.0.19	All	All	All
Application	Oracle	Mysql	5.0.3	beta	All	All
Application	Oracle	Mysql	5.0.6	All	All	All
Application	Oracle	Mysql	5.0.7	All	All	All
Application	Oracle	Mysql	5.0.8	All	All	All
Application	Oracle	Mysql	5.0.9	All	All	All

cpe:2.3:a:mysql:mysql:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.16:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.17:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.20:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.3:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.4:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.5:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.1:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.10:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.15:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.16:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.17:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.2:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.20:*:*:*:*:*:*:*:

cpe:2.3:a:mysql:mysql:5.0.3:*:*:*:*:*:*:*

cpe:2.3:a:mysql:mysql:5.0.4:*:*:*:*:*:*:*

cpe:2.3:a:mysql:mysql:5.0.5:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.0:alpha:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.11:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.12:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.13:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.14:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.18:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.19:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.3:beta:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.6:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.7:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.8:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.9:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.0:alpha:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.11:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.12:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.13:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.14:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.18:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.19:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.3:beta:*:*:*:*:*:*:

cpe:2.3:a:oracle:mysql:5.0.6:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.7:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.8:*:*:*:*:*:*:*

cpe:2.3:a:oracle:mysql:5.0.9:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report