

[USN-274-2] MySQL vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-05/msg00275.html>

- *From:* Martin Pitt <martin.pitt@xxxxxxxxxxxxxx>
 - *Date:* Mon, 15 May 2006 16:38:26 +0200
-

=====
Ubuntu Security Notice USN-274-2 May 15, 2006
mysql-dfsg vulnerability
CVE-2006-0903
=====

A security issue affects the following Ubuntu releases:

Ubuntu 5.04 (Hoary Hedgehog)
Ubuntu 5.10 (Breezy Badger)

The following packages are affected:

mysql-server

The problem can be corrected by upgrading the affected package to version 4.0.23-3ubuntu2.4 (for Ubuntu 5.04), or 4.0.24-10ubuntu2.3 (for Ubuntu 5.10). In general, a standard system upgrade is sufficient to effect the necessary changes.

Details follow:

USN-274-1 fixed a logging bypass in the MySQL server. Unfortunately it was determined that the original update was not sufficient to completely fix the vulnerability, thus another update is necessary. We apologize for the inconvenience.

For reference, these are the details of the original USN:

A logging bypass was discovered in the MySQL query parser. A local attacker could exploit this by inserting NUL characters into query strings (even into comments), which would cause the query to be logged incompletely.

This only affects you if you enabled the 'log' parameter in the MySQL configuration.

Updated packages for Ubuntu 5.04:

[USN-274-2] MySQL vulnerability

Source archives:

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/mysql-dfsg_4.0.23-3ubuntu2.4.diff.gz

Size/MD5: 347218 5bf62963f2439449d17429b974dc954e

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/mysql-dfsg_4.0.23-3ubuntu2.4.dsc

Size/MD5: 891 cf807937ea7cb09d1717c562c355e2cd

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/mysql-dfsg_4.0.23.orig.tar.gz

Size/MD5: 9814467 5eec8f66ed48c6ff92e73161651a492b

Architecture independent packages:

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg/mysql-common_4.0.23-3ubuntu2.4_all.deb

Size/MD5: 32366 1a3bd9d864cae3bfa1987f859b5624aa

amd64 architecture (Athlon64, Opteron, EM64T Xeon)