

[Full-disclosure] [USN-440-1] MySQL vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2007-03/msg00385.html>

- *From:* Kees Cook <kees@xxxxxxxxxx>
 - *Date:* Wed, 21 Mar 2007 19:15:38 -0700
-

=====
Ubuntu Security Notice USN-440-1 March 21, 2007
mysql-5.0 vulnerability
CVE-2007-1420
=====

A security issue affects the following Ubuntu releases:

Ubuntu 6.06 LTS
Ubuntu 6.10

This advisory also applies to the corresponding versions of
Kubuntu, Edubuntu, and Xubuntu.

The problem can be corrected by upgrading your system to the
following package versions:

Ubuntu 6.06 LTS:
mysql-server-5.0 5.0.22-0ubuntu6.06.3

Ubuntu 6.10:
mysql-server-5.0 5.0.24a-9ubuntu0.1

In general, a standard system upgrade is sufficient to effect the
necessary changes.

Details follow:

Stefan Streichbier and B. Mueller of SEC Consult discovered that MySQL
subselect queries using "ORDER BY" could be made to crash the MySQL
server. An attacker with access to a MySQL instance could cause an
intermittant denial of service.

Updated packages for Ubuntu 6.06 LTS:

Source archives:

[Full-disclosure] [USN-440-1] MySQL vulnerability

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg-5.0/mysql-dfsg-5.0_5.0.22-0ubuntu6.06.3.diff.gz

Size/MD5: 127117 30ac47cfd02a983b7ae79232ecd6d86d

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg-5.0/mysql-dfsg-5.0_5.0.22-0ubuntu6.06.3.dsc

Size/MD5: 1107 87d6c9fc492af83f792f56d8f503f94d

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg-5.0/mysql-dfsg-5.0_5.0.22.orig.tar.gz

Size/MD5: 18446645 2b8f36364373461190126817ec872031

Architecture independent packages:

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg-5.0/mysql-client_5.0.22-0ubuntu6.06.3_all.deb

Size/MD5: 37034 2701d0790885aa42c241bb17b1b41ef5

http://security.ubuntu.com/ubuntu/pool/main/m/mysql-dfsg-5.0/mysql-common_5.0.22-0ubuntu6.06.3_all.deb