

# [Full-Disclosure] Proofpoint Protection Server remote MySQL root user vulnerability

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-02/1251.html>

---

*From:* anony mous ([auto355649\\_at\\_hushmail.com](mailto:auto355649_at_hushmail.com))

*Date:* 02/22/04

To: [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)  
Date: Sat, 21 Feb 2004 19:09:10 -0800

Product: Protection Server  
Version: unknown/Red Hat Linux  
Developer: Proofpoint  
URL: [www.proofpoint.com](http://www.proofpoint.com)

## Summary:

The MySQL server may be remotely access by the "root" user without using a password.

## Details:

The Proofpoint Protection Server is a software product to filter spam and other e-mail traffic. It's installed on Red Hat Linux. A partial customer list may be found on their website.

By default, the embedded MySQL 4.0 server binds to the default port (3306/tcp) on every IP. The software has no packet filtering or port restrictions of it's own, so all bound ports are wide open to the network.

The specific flaw is that the "root" user in MySQL is not restricted from connecting from any host ('%') and additionally the root user HAS NO PASSWORD. There are a few minor restrictions on the root user when logging in from a remote host, such as no Reload\_priv (more on this later), but basic functions like INSERT and DELETE are allowed.

Exploiting this is as easy as  
`$ mysql -u root -h a.b.c.d`

From there you can view contents of the different databases, including dumping the hashed passwords for any of the password-protected users. You can then run one of the brute-force MySQL password hash crackers against them (it's the old-style 16byte hashes).

It is also possible to create new users indirectly by INSERT'ing into the user table for database mysql. Remote root will not be able to FLUSH

## Full-Disclosure: [Full-Disclosure] Proofpoint Protection Server remote MySQL root user vulnerability

PRIVILEGES (required to make the user active—this is because no Reload\_priv), but if the database is restarted for any reason those users will become active and able to authenticate. Remote root also has the ability to delete users.

More destructive operations were not tested due to the accidental nature of discovery, but use your imagination (certainly a DoS is possible simply by deleting users required by the system). Also since the systems are running on Red Hat, it may be possible to exploit one of several recent vulnerabilities in the Linux 2.4 kernel through MySQL.

Concerned about your privacy? Follow this link to get FREE encrypted email: <https://www.hushmail.com/?l=2>

Free, ultra-private instant messaging with Hush Messenger  
<https://www.hushmail.com/services.php?subloc=messenger&l=434>

Promote security and make money with the Hushmail Affiliate Program:  
<https://www.hushmail.com/about.php?subloc=affiliate&l=427>

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>