

WineHQ database compromise

By *srlinuxx*

Created *12/10/2011 - 6:00am*

Submitted by srlinuxx on Wednesday 12th of October 2011 06:00:10 AM Filed under [Software](#) [1] [Security](#) [2] [Web](#) [3]

I am sad to say that there was a compromise of the WineHQ database system.

What we know at this point that someone was able to obtain unauthorized access to the phpmyadmin utility. We do not exactly how they obtained access; it was either by compromising an admins credentials, or by exploiting an unpatched vulnerability in phpmyadmin.

We had reluctantly provided access to phpmyadmin to the appdb developers (it is a very handy tool, and something they very much wanted). But it is a prime target for hackers, and apparently our best efforts at obscuring it and patching it were not sufficient.

So we have removed all access to phpmyadmin from the outside world.

We do not believe the attackers obtained any other form of access to the system.

[Rest here](#) [4]

[Software Security Web](#)

Source URL: <http://www.tuxmachines.org/node/55155>

Links:

[1] <http://www.tuxmachines.org/taxonomy/term/38>

[2] <http://www.tuxmachines.org/taxonomy/term/59>

[3] <http://www.tuxmachines.org/taxonomy/term/103>

[4] <http://www.winehq.org/pipermail/wine-users/2011-October/097753.html>