

## Re: [Full-Disclosure] Re: IRCXpro 1.0 – Clear local and default remote admin passwords

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-06/0043.html>

---

*From:* Darren Reed ([avalon\\_at\\_caligula.anu.edu.au](mailto:avalon_at_caligula.anu.edu.au))

*Date:* 06/03/03

To: [support@ircxpro.com](mailto:support@ircxpro.com) (IRCXpro Support)

Date: Wed, 4 Jun 2003 01:56:35 +1000 (Australia/ACT)

In some mail from IRCXpro Support, sie said:

>

> *Reply to Feedback from Darren:*

>

>> *Firstly, there has been support for storing passwords, encrypted, in*

>> *configuration files on Unix for over 10 years, if not longer. I can*

>

> *The reason why IRC servers "IRCD.config" files don't use encryption (see*

> *file attachment for example) is because 49 times out of 50 they do not come*

> *with a GUI program. Administrators main method of changing the*

> *configuration is to manually edit the file using a notepad utility.*

The free IRC servers for Unix have never shipped with a gui and this has never stopped them from supporting encrypted passwords. Are you justifying lesser programming practises just because you're developing for Windows?

>> *at leisure. Windows, Linux, it does not matter, there are security*

>> *threats to all environments that when exploited given outsiders some*

>> *sort of "local access".*

>

> *Then in this case this would be an operating system vulnerability.*

And this never happens, does it?

Or, lets use another example, what if someone used your software on a system that was using microsoft's terminal service packages or something citrix like where a central server does support multiple users ? The users' whose passwords are being stored by your software might be remote in this case but what of the real users? Yes, an extreme case and equally unlikely, but you never know...

> *Overuse in the use of encrypted passwords can be counter productive to*

> *functionality.*

Really ?

- > *There are good reasons to keep passwords clear text passwords to better interface with other software.*
- > *For example Merak Mail server software*
- > *([http://www.icewarp.com/Products/Merak\\_Email\\_Server\\_Software/](http://www.icewarp.com/Products/Merak_Email_Server_Software/))*
- > *When using this mail server, it can store the accounts on an SQL Server.*
- > *The passwords are stored clear text. This enables other software to interface with its data to create and sync its accounts/passwords with other systems.*

Sounds like a poorly designed authentication interface, to me, where real security was not given due consideration and an "obvious" solution used despite the compromise to security that results. Maybe there'll be something about them in an upcoming email to full-disclosure/bugtraq, lampooning them for similarly poor design choices and implementation that introduces unnecessary security risks.

- > *However we will give the issue raised due attention in our next version*
- > *release and appreciate everybody's efforts & feedback to further improving*
- > *our product.*

That's good to hear.

Cheers,  
Darren

---

Full-Disclosure – We believe in it.  
Charter: <http://lists.netsys.com/full-disclosure-charter.html>