LibpreludeDB - Bug #392

Potential security risc in preludedb-admin?

01/15/2011 03:37 PM - Paul Buetow

Status:	Assigned	**Start date:**	01/15/2011
Priority:	Normal	**Due date:**	
Assignee:	Francois POIROTTE	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:			
Resolution:			

Description

Hi!

I wanted to ask a question regarding preludedb-admin.

I am using 0.9.14.1-2 (Debian GNU/Linux Lenny). There is no way not to define the database password (e.g. mysql password) NOT in the command line argument. The password shows up in plain text in the system process list while using preludedb-admin.

It should be possible to "pipe" the arguments to preludedb-admin

The current way:

preludedb-admin delete alert "type=mysql name=prelude user=prelude pass=prelude" --criteria "alert.create_time < $DATE"

"Better way":

some-script-generating-arguments | preludedb-admin

(Alternatively just pipe the "type=mysql name=prelude user=prelude" part)

And / Or:

preludedb-admin --args filename

(Alternatively just read the "type=mysql name=prelude user=prelude" part from file)

And / Or:

Read password from an environment variable:

#/bin/sh

export PRELUDE_PASS=prelude
exec preludedb-admin delete alert "type=mysql name=prelude user=prelude" --criteria "alert.create_time < $DATE"

And / Or:

Read password from stdin if missing in the argument.

Hope you got my point smile.png

Thanks a lot and best regards,

History

#1 - 02/08/2012 08:14 PM - Francois POIROTTE

- Status changed from New to Assigned

- Assignee set to Francois POIROTTE

Faut que je retrouve la commande exacte, mais il existe un

#2 - 05/31/2012 05:07 PM - Jean-Charles ROGEZ

- Project changed from PRELUDE SIEM to LibpreludeDB

- Category deleted (generic)