

Re: ODBC Login information saved as plain text... :(

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0300.html>

From: Deus, Attonbitus (*Thor_at_HammerofGod.com*)

Date: 07/23/03

Date: Wed, 23 Jul 2003 07:57:34 -0700

To: hanez <mailman@hanez.org>, bugtraq@securityfocus.com

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

At 01:30 AM 7/22/2003, hanez wrote:

>(this is my second post of this mail because the first didn't

>arrived to the list...)

>

>Hello All,

>

>i have found an interesting thing in Windows XP. When i create an
>ODBC SYSTEM-DSN (Datasource available for all users) for accessing a
>SQL-Server, it is saved in the Windows Registry. The Problem there
>is, that Windows is saving the login information like username and
>password as plain text in the registry keys and every user who has
>access to this PC could read these entries.

Please note that this has nothing to do with Windows XP, or Win2k,
etc. It

has to do with the ODBC driver you have chosen to use. See below.

>I don't have big problems with this but i think that many developers
>are using
>this for building database driven applications. If these
>applications are running on client PC's where noone should know the
>passwords of the database server, every user could read the login
>information in the Windows registry and then use an application like
>MS-Access to get access to the tables stored on the server. I think
>this is a very insecure thing! Users could get Information about the
>structures of the tables on the database server and maybe if not
>correct configured get write access to all tables... A horrible
>thing i think...

Then it is the developers fault. Using "mixed-mode" type
applications is
not a secure method of accessing a database. This would be no

Re: ODBC Login information saved as plain text... :(

SecurityFocus Bugtraq: Re: ODBC Login information saved as plain text... :(

different
than someone having a client-side application that made direct ADODB
calls
to a database and included the logon credentials in the connection
string-
same with .asp and so forth.

*>I have only tested this on my Windows XP workstation and one and
>only Windows machine, so i could not test it on other versions of
>this stupid OS. Like i'm knowing M\$ it is a problem in all versions
>of Windows. Windows simply is a big security problem...*

Not to be crass, but the "big problem" is that you have not performed
adequate research. To be honest, this smacks of one of those BT
posts
specifically written to be able to say things like "stupid OS" and so
forth. One should note that a Perl script written on Linux to access
a SQL
server back end would still have the creds stored in plain-text
unless the
developer chose to better secure it. And we won't even get into
netmon
sniffing of en-encrypted sessions. As far as the permissions go, of
course
all users can read a system DSN- IT IS A SYSTEM DSN! If the
developer
really cares, he can create User DSN's, which are created in the
HKEY_USERS
hive with restricted permissions and cloned to the HKEY_CURRENT_USER
hive
with admin/specific user permissions. But they don't do that. They
create
single user accounts and share them among all the users. Guess whose
fault
that is?? Yep, the DEVELOPER.

```
>[HKEY_LOCAL_MACHINE\SOFTWARE\ODBC\ODBC.INI\TESTDSN]
>
>"Driver"="C:\\WINDOWS\\System32\\myodbc3.dll"
>
>"Description"="MySQL ODBC 3.51 Driver DSN"
>
>"Database"="test"
>
>"Server"="192.168.0.1"
>
>"User"="user_name"
>
>"Password"="plain_password"
>
>"Port"="3306"
```

Re: ODBC Login information saved as plain text... :(

SecurityFocus Bugtraq: Re: ODBC Login information saved as plain text... :(

```
>  
>"Option"="3"  
>  
>"Stmt"=""  
>//end
```

This is because your MySQL ODBC driver was *written to do this.*
This is
how MySQL *wants* the data. In contrast, if you were using MS
SQLServer,
and insisted on using mixed-mode authentication, where you connect up
with
a specific user account and created such a system DSN, even when you
connect up and test, the reg entry only stores the following:

```
"Driver = %SystemDrive%\%WinDir%\System32\sqlsrv32.dll"  
"LastUser = Dude"  
"Server = ServerName"
```

When you attempt to establish a connection via the System DSN, you
are
prompted for your username and password- again, this is a result of
how the
ODBC driver was written.
This issue has nothing to do with Windows XP being a "stupid OS."
That
distinction lies elsewhere.

hth

T

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0

```
iQA/AwUBPx6iYohsmyD15h5gEQKnRQCgnNiN7yAjkVsjtO0x+g7dv1LFaRcAoPPc  
k8fVkyalOd+tTAZyq1//Bqtm  
=16u1
```

-----END PGP SIGNATURE-----

Re: ODBC Login information saved as plain text... :(