

[NT] Microsoft JET Database Engine 4.0 Buffer Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-07/0059.html>

From: SecuriTeam (*support_at_securiteam.com*)

Date: 07/16/03

To: list@securiteam.com

Date: 16 Jul 2003 10:05:41 +0200

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

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Microsoft JET Database Engine 4.0 Buffer Overflow

SUMMARY

Microsoft JET database engine is a database management system that retrieves data from and stores data in user and system databases. The Microsoft Jet database engine can be thought of as a data manager upon which database systems, such as Microsoft Access, are built.

Microsoft Jet database engine has sophisticated query and optimization capabilities that are unmatched by other desktop database engines in its class. These features include updatable views, heterogeneous joins, and the ability to work seamlessly with a wide variety of industry-standard database formats. The Microsoft Jet query engine is designed to accept user requests for information or action in the form of Structured Query Language (SQL) statements. Microsoft Jet parses, analyzes, and optimizes these queries, and either returns the resulting information in the form of a Recordset object or performs the requested action.

Although Microsoft Jet borrows many query techniques from client/server

Securiteam: [NT] Microsoft JET Database Engine 4.0 Buffer Overflow

relational database management systems (DBMSs) such as Microsoft SQL Server, it remains a file-server database. All queries are processed on individual workstations running copies of a host application, such as Microsoft Access, or a custom application created by using a tool, such as Microsoft Visual Basic. Microsoft Jet does not act as a true database server, such as SQL Server, that process data requests independently of the application requesting data. However, Microsoft Jet can send queries to SQL Server or other ODBC database servers for processing.

Microsoft Jet Database Engine provides support for many databases types such as *.mdb(MS Access), *.xls(MS Excel), *.txt (text files), *.dbf (dBase), etc. Microsoft Jet Database Engine allows the use of Visual Basic for Applications (VBA) functions and SQL aggregated functions in SQL statements, when a SQL query is executed and a long function name is supplied a Unicode stack based overflow occurs.

DETAILS

Vulnerable systems:

- * Microsoft SQL Server 2000
- * SQL Server version 7
- * MSDE
- * All software using MS Jet Engine Service Pack 6

Example:

```
Select XXX...()  
(XXX... more than 276 chars)
```

Microsoft SQL Server allows to access remote data from an OLE DB data source using OpenRowset(), Opendatasource(), Openquery() and Linked Servers. When querying remote data sources using JET 4.0 OLE DB provider and a long function name is specified a Unicode stack based overflow occurs:

```
select * from  
openrowset('microsoft.jet.oledb.4.0','c:\anydatabase.mdb';'admin';','select XXX...())
```

Alternatively,

```
select * from Openquery(SomeJet40LinkedServer,'Select XXX...()')  
(XXX... more than 276 chars)
```

When the vulnerability is exploited to run arbitrary code on SQL Server, the code will run in the context of the SQL Server service account. On the latest SQL Server, the Microsoft Jet OLE DB provider is disabled by default, but it is not uncommon to find servers with the provider enabled or with a linked server to a supported Microsoft Jet database.

Workaround:

On SQL Server make sure you have Microsoft Jet OLE DB provider disabled. Check the value DisallowAdhocAccess under key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft SQL Server\InstanceNameHere\Providers\Microsoft.Jet.OLEDB.4.0

Securiteam: [NT] Microsoft JET Database Engine 4.0 Buffer Overflow

Value must not exist or be set to 1.

Vendor Status:

Microsoft was contacted and they release a fix in MS Jet 4.0 Service Pack 7.

Patch Availability:

Under the <<http://windowsupdate.microsoft.com>>

<http://windowsupdate.microsoft.com> web page, there is a link for the Jet 4.0 SP7 (under Recommended Updates as 282010: Recommended Update for Microsoft Jet 4.0 Service Pack 7 (SP7))

ADDITIONAL INFORMATION

The information has been provided by <<mailto:cesarc56@yahoo.com>> Cesar.

=====

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.