

Microsoft JET Database Engine 4.0 buffer overflow.

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-07/0038.html>

From: Cesar (*cesarc56_at_UOL.COM.AR*)

Date: 07/15/03

Date: Mon, 14 Jul 2003 20:26:16 -0300

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Security Advisory

Name: Microsoft JET Database Engine 4.0 buffer overflow.

System Affected : Microsoft SQL Server 2000, SQL Server 7 & MSDE.

All software using MS Jet Engine Service Pack 6 (and prior?) are vulnerable.

Severity : High

Remote exploitable : Yes

Author: Cesar Cerrudo.

Date: 07/11/03

Advisory Number: CC070306

Legal Notice:

This Advisory is Copyright (c) 2003 Cesar Cerrudo.

You may distribute it unmodified and for free. You may NOT modify it and distribute it or distribute parts of it without the author's written permission. You may NOT use it for commercial intentions (this means include it in vulnerabilities databases, vulnerabilities scanners, any paid service, etc.) without the author's written permission. You are free to use Microsoft details for commercial intentions.

Disclaimer:

The information in this advisory is believed to be true though it may be false.

The opinions expressed in this advisory are my own and not of any company. The usual standard disclaimer applies, especially the fact that Cesar Cerrudo is not liable for any damages caused by direct or indirect use of the information or functionality provided by this advisory.

Cesar Cerrudo bears no responsibility for content or misuse of this advisory or any derivatives thereof.

Overview:

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.

NT–Bugtraq: Microsoft JET Database Engine 4.0 buffer overflow.

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 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 doesn't 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.

Details:

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 Aplicaciones (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:

```
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...())
```

or

```
select * from Openquery(SomeJet40LinkedServer,'Select XXX...()')
```

etc.

(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 latest SQL Server versions Microsoft Jet OLE DB provider is disabled by default, but it's not uncommon to find servers with the provider enabled or with a linked server

NT-Bugtraq: Microsoft JET Database Engine 4.0 buffer overflow.

to a supported Microsoft Jet database.

This vulnerability can be exploited to run arbitrary code. It can be exploited using SQL Injection most probably against MS Access databases or SQL Server, also Web applications that allow users to submit arbitrary SQL queries values are vulnerable.

On SQL Server if Microsoft Jet OLE DB provider has been enabled or there is a Linked Server to a Microsoft Jet supported database any SQL Server user will be able to exploit this vulnerability.

Tries and exploitation of this vulnerability in web applications using Active Server Pages (ASP) with Microsoft Jet Engine, could cause IIS 5.0 (not tested in other IIS versions but they may have the same behaviour) to stop processing Active Server Pages (ASP).

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

value must not exist or be 1.

Vendor Status:

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

Patch Available :

Important Note: THE FIX IS NOT INCLUDED IN CRITICAL UPDATES

Go to <http://windowsupdate.microsoft.com>

The link for the Jet 4.0 SP7 download is listed under Recommended Updates as 282010: Recommended Update

for Microsoft Jet 4.0 Service Pack 7 (SP7)

NEW SECURITY LIST!!!: For people interested in SQL Server security, vulnerabilities, SQL injection, etc. Get advisories and vulnerabilities before!!!

Join at:

sqlserversecurity-subscribe@yahoogroups.com

<http://groups.yahoo.com/group/sqlserversecurity/>

oo

Are You "Certifiable"? Summer's Hottest Certification Just Got HOTTER!

