

AppSecInc Security Alert: Buffer Overflow in UDP broadcasts for Microsoft SQL Server client utilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-08/0311.html>

From: Aaron C. Newman (aaron_at_newman-family.com)

Date: 08/21/03

To: <bugtraq@securityfocus.com>, "'Windows NTBugtraq Mailing List'" <NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM>

Date: Thu, 21 Aug 2003 14:59:21 -0400

Buffer Overflow in UDP broadcasts for Microsoft SQL Server client utilities

Risk level: High

Summary:

A Unicode buffer overflow exists in MDAC which is used by the SQL Server SQL-DMO library that could allow a remote user to execute malicious code on the target computer. The vulnerability does not occur when accepting incoming connections, but rather in the response to broadcast queries.

Details:

One of the features of the SQL Server network libraries is the ability to query a list of SQL Servers on the local network. This is accomplished by sending a UDP broadcast on port 1434 which will reach all applications on the local subnet. This function is a component of SQL-DMO which is used by the SQL Server Service Manager (whenever it is started), Enterprise Manager (when registering a server), Query Analyzer and SQL Profiler (when clicking "..." button), DTS (when selecting a SQL Server), etc...

All SQL Servers receiving the broadcast request respond with a standard UDP packet. If a malicious machine responds to this broadcast with an overlong packet a stack buffer overflow occur. The overflow occurs in a UNICODE string, so the Venetian method of performing a buffer overflow would

need to be used to exploit this vulnerability. There is a white paper from Chris Ansley on how this is done, as well as a presentation from Dave Aitel.

Any SQL Server utilities that use the SQL-DMO function to retrieve a list of SQL Servers will be vulnerable to this attack. An attack is not mounted directly against the target. Instead an attacker could attempt several methods of exploiting the vulnerability:

- 1) Setup a service listening for data on UDP port 1434 and responding with the attack payload whenever data is received. This network would require being on the same subnet.
- 2) Bombarding a remote subnet with UDP attack packets waiting for someone to query the network. For example, send the attack packet every 2 seconds to 192.168.3.255 will reach all machines on the 192.168.3.x subnet. When someone finally does send a UDP broadcast, they will accept this packet and be exploited. This method would take a bit of luck, persistence, or some social engineering.
- 3) It may also be possible for a non-privileged login in MS SQL to cause the SQL Server to send out a query request directly to an IP Address on the network. The following SQL statement causes the SQL Server to query a host named SERVER with a UDP packet:

```
SELECT * FROM openrowset( 'SQLOLEDB', 'server=SERVER\instance
name;uid=sa;pwd=' , ")
```

However, on our systems, we were unable to trigger the overflow from the response. There may be other methods to cause the SQL Server to send the UDP query and trigger the overflow.

One of the features of SQL Server which makes this vulnerability simpler to exploit is that the SQL Server Service Manager queries the network using SQL-DMO every time it starts which happens when a user with the SQL Server client utilities logs into Windows. This would occur anytime someone logged into the Windows server on which SQL Server is installed, or anytime a database administrator logs into his or her machine.

Links:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0353>

<http://www.microsoft.com/technet/security/bulletin/MS03-033.asp>

Fix:

This vulnerability affects the following packages:

Microsoft Data Access Components 2.7 SP1

Microsoft Data Access Components 2.7

Microsoft Data Access Components 2.6 SP2

Microsoft Data Access Components 2.5 SP3

Microsoft Data Access Components 2.5 SP2

If you have one of these packages installed, apply the hot fix from

<http://support.microsoft.com/default.aspx?scid=kb;en-us;823718>.

Acknowledgement:

Thanks to Cesar Cerrudo for researching this vulnerability!

Thank you,

support@appsecinc.com

Application Security, Inc.

SecurityFocus Bugtraq: AppSecInc Security Alert: Buffer Overflow in UDP broadcasts for Microsoft SQL Server client utilities

phone: 212-420-9270

fax: 212-420-9680

-Protection Where It Counts-