

[NT] Buffer Overrun in MDAC Function Could Allow Code Execution (MS04-003)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-01/0047.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 01/14/04

To: list@securiteam.com

Date: 14 Jan 2004 11:50:56 +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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

Buffer Overrun in MDAC Function Could Allow Code Execution (MS04-003)

SUMMARY

Microsoft Data Access Components (MDAC) is a collection of components that provides the underlying functionality for a number of database operations, such as connecting to remote databases and returning data to a client. When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. Because of a vulnerability in a specific MDAC component, an attacker could respond to this request with a specially-crafted packet that could cause a buffer overflow.

An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. The actions an attacker could carry out would be dependent on the permissions under which the program using MDAC ran. If the program ran with limited privileges, an attacker would be limited accordingly; however, if the program ran under the local system context, the attacker would have the same level of permissions.

Since the original version of MDAC on your system may have changed from

Securiteam: [NT] Buffer Overrun in MDAC Function Could Allow Code Execution (MS04-003)

updates available on the Microsoft Web site, we recommend using the following tool to determine the version of MDAC you have on your system: Microsoft Knowledge Base article 301202 "HOW TO: Check for MDAC Version" discusses this tool and explains how to use it. In addition, Microsoft Knowledge Base article 231943 discusses the release history of the different versions of MDAC.

DETAILS

Affected Software:

- * Microsoft Data Access Components 2.5 (included with Microsoft Windows 2000)
- * Microsoft Data Access Components 2.6 (included with Microsoft SQL Server 2000)
- * Microsoft Data Access Components 2.7 (included with Microsoft Windows XP)
- * Microsoft Data Access Components 2.8 (included with Microsoft Windows Server 2003)

Note The same update applies to all these versions of MDAC –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=39472EE8-C14A-47B4-BFCC-87988E062D91&disp=1>
Download the Update

* Microsoft Data Access Components 2.8 (included with Windows Server 2003 64-Bit Edition) –

<http://www.microsoft.com/downloads/details.aspx?FamilyId=1D93D9E4-2B22-4595-B8C5-643824857EC0&disp=1>
Download the Update

Mitigating factors:

* For an attack to be successful an attacker would have to simulate a SQL server that is on the same IP subnet as the target system.

* When a client system on a network tries to see a list of computers that are running SQL Server and that reside on the network, it sends a broadcast request to all the devices that are on the network. A target system must initiate such a broadcast request to be vulnerable to an attack. An attacker would have no way of launching this first step but would have to wait for anyone to enumerate computers that are running SQL Server on the same subnet. In addition, a system is not vulnerable by having these SQL management tools installed.

* Code executed on the client system would only run under the privileges of the client program that made the broadcast request.

Workarounds

Microsoft has tested the following workarounds. These workarounds will not correct the underlying vulnerability. However, they help block known attack vectors. Workarounds may reduce functionality in some cases; in such cases, the reduction in functionality is identified below.

Securiteam: [NT] Buffer Overrun in MDAC Function Could Allow Code Execution (MS04-003)

Block UDP port 1434 from accepting inbound traffic.

Block UDP port 1434 on your system's network interface from accepting inbound traffic. For example, to block network traffic that originates from a Windows 2000-based computer that comes from UDP 1434 to this host, type the following at the command line:

```
ipsecpol -w REG -p "Block UDP 1434 Filter" -r "Block Inbound UDP 1434 Rule" -f *=0:1434:UDP -n BLOCK -x
```

See Microsoft Knowledge Base article 813878 "How to Block Specific Network Protocols and Ports by Using IPSec" for more information about IPSec and the technology that this workaround uses.

Impact of Workaround:

SQL client systems would no longer be able to initiate SQL broadcast requests. For example, tools like SQL Enterprise Manager use broadcast requests to enumerate all SQL Server instances on a subnet. The workaround would also prevent connections to non-default instances of SQL Server. An example of non-default instances of SQL server is additional instances of SQL server that are installed on the same computer.

Frequently Asked Questions

What is the scope of the vulnerability?

This is a buffer overrun vulnerability. An attacker who successfully exploited this vulnerability could gain the same level of privileges over the system as the program that initiated the broadcast request. The actions that an attacker could carry out on the system would depend on the permissions of the user account under which the program using MDAC ran.

If the program ran with limited privileges, an attacker would be limited accordingly. However, if the program ran under the context of Local System, the attacker could gain the same level of permissions.

What causes the vulnerability?

The vulnerability results because of an unchecked buffer in a specific MDAC component. If an attacker were able to successfully exploit this vulnerability, it could allow them to gain control over the system and take any action that the legitimate process executing MDAC could take.

What is Microsoft Data Access Components?

Microsoft Data Access Components (MDAC) is a collection of components that make it easy for programs to access databases and to change the data within them. Modern databases may take a variety of forms (for example, SQL Server databases, Microsoft Access databases, and XML files) and may be housed in a variety of locations (for example, on the local system or on a remote database server).

MDAC provides a consolidated set of functions for working with these data sources in a consistent manner. A good discussion of MDAC and the components that it provides is available on MSDN.

Do I have MDAC on my system?

It is very likely that you do because MDAC is a ubiquitous technology:

- * MDAC installs as part of Windows 2000, SQL Server 2000, Windows XP, and Windows Server 2003.

- * MDAC is available for download from the Microsoft Web site.

- * MDAC is installed by many other Microsoft programs. To name just a few cases, it is installed as part of the Microsoft Windows NT 4.0 Option Pack, Microsoft Access, and SQL Server.

A tool is available that can help you determine what version of MDAC is running on your system. Microsoft Knowledge Base article 301202 "HOW TO: Check for MDAC Version" describes this tool and explains how to use it. Also, Microsoft Knowledge Base article 231943 discusses the release history of the different versions of MDAC.

Why did Microsoft Windows Update offer me a language version of the security update that is different than I expected?

It is recommended, but not necessary, to install the language version of this update that follows the MDAC language that the customer has installed. Customers download this security update by using Windows Update, and subsequently by using Microsoft Software Update Services (SUS), based on the language version of Windows that a customer has.

A customer could have a more recent version of MDAC installed, which is localized into a language other than the language of the instance of Windows. For example, if a customer installs a Spanish language instance of SQL Server installed on an English instance of Windows, the customer may have a Spanish language version of MDAC installed. This is a supported configuration for which we would recommend the Spanish language update. Certain log entries note the disparity. If the customer prefers the Spanish update, they should install the security update by using the download links that are at the beginning of this security bulletin.

Note: While the installation of this security update is in English, the security update in itself is localized and Windows Update will offer customers an update that match the language version of Windows they have.

What might an attacker use the vulnerability to do?

This vulnerability could enable an attacker to reply to a client system request with a malformed User Datagram Protocol (UDP) packet, which would cause a buffer overrun to occur. If an attacker were to successfully exploit this vulnerability, they could take any action that they wanted to on the system that the overrun process could take.

How could an attacker exploit this vulnerability?

An attacker could exploit this vulnerability by simulating a server running SQL Server that listens on a network for a client system to request an enumeration of all systems on the specific network that are running SQL Server. By replying to that request with a specially-crafted packet, an attacker could cause a buffer overrun to occur in a specific

Securiteam: [NT] Buffer Overrun in MDAC Function Could Allow Code Execution (MS04-003)

MDAC component on the client system.

What does the update do?

This security update removes the vulnerability by validating that the number of bytes that are specified in the reply is of an appropriate value.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Product Security.

=====

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.