

Alert: Microsoft Security Bulletin – MS02–065

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-11/0014.html>

From: Russ (Russ.Cooper@RC.ON.CA)

Date: 11/20/02

Date: Wed, 20 Nov 2002 12:30:40 -0500

From: Russ <Russ.Cooper@RC.ON.CA>

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

<http://www.microsoft.com/technet/security/bulletin/MS02-065.asp>

Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)

Originally posted: November 20, 2002

Summary

Who should read this bulletin: Customers using Microsoft® Windows®, particularly those who operate web sites or browse the Internet.

Impact of vulnerability: Run code of attacker's choice

Maximum Severity Rating: Critical

Recommendation: Users should apply the patch immediately.

Affected Software:

- Microsoft Data Access Components (MDAC) 2.1
- Microsoft Data Access Components (MDAC) 2.5
- Microsoft Data Access Components (MDAC) 2.6
- Microsoft Internet Explorer 5.01
- Microsoft Internet Explorer 5.5
- Microsoft Internet Explorer 6.0

Note: The vulnerability does not affect Windows XP, despite the fact that it uses Internet Explorer 6.0. Windows XP customers do not need to take any action.

End User Bulletin: An end user version of this bulletin is available at:

http://www.microsoft.com/security/security_bulletins/ms02-065.asp

Technical description:

Microsoft Data Access Components (MDAC) is a collection of components used to provide database connectivity on Windows platforms. MDAC is a ubiquitous technology, and it is likely to be present on most Windows systems:

NT–Bugtraq: Alert: Microsoft Security Bulletin – MS02–065

- It is included by default as part of Windows XP, Windows 2000, and Windows Millennium.
- It is available for download as a stand–alone technology in its own right
- It is either included in or installed by a number of other products and technologies. For instance, MDAC is included in the Windows NT® 4.0 Option Pack, and some MDAC components are present as part of Internet Explorer even if MDAC itself is not installed.

MDAC provides the underlying functionality for a number of database operations, such as connecting to remote databases and returning data to a client. One of the MDAC components, known as Remote Data Services (RDS), provides functionality that support three–tiered architectures – that is, architectures in which a client's requests for service from a back–end database are intermediated through a web site that applies business logic to them. A security vulnerability is present in the RDS implementation, specifically, in a function called the RDS Data Stub, whose purpose it is to parse incoming HTTP requests and generate RDS commands.

A security vulnerability resulting from an unchecked buffer in the Data Stub affects versions of MDAC prior to version 2.7 (the version that shipped with Windows XP). By sending a specially malformed HTTP request to the Data Stub, an attacker could cause data of his or her choice to overrun onto the heap. Although heap overruns are typically more difficult to exploit than the more–common stack overrun, Microsoft has confirmed that in this case it would be possible to exploit the vulnerability to run code of the attacker's choice on the user's system.

Both web servers and web clients are at risk from the vulnerability:

- Web servers are at risk if a vulnerable version of MDAC is installed and running on the server. To exploit the vulnerability against such a web server, an attacker would need to establish a connection with the server and then send a specially malformed HTTP request to it, that would have the effect of overrunning the buffer with the attacker's chosen data. The code would run in the security context of the IIS service (which, by default, runs in the LocalSystem context)
- Web clients are at risk in almost every case, as the RDS Data Stub is included with all current versions of Internet Explorer and there is no option to disable it. To exploit the vulnerability against a client, an attacker would need to host a web page that, when opened, would send an HTTP reply to the user's system and overrun the buffer with the attacker's chosen data. The web page could be hosted on a web site or sent directly to users as an HTML Mail. The code would run in the security context of the user.

Clearly, this vulnerability is very serious, and Microsoft recommends that all customers whose systems could be affected by them take appropriate action immediately.

- Customers using Windows XP, or who have installed MDAC 2.7 on their systems are at no risk and do not need to take any action.
- Web server administrators who are running an affected version of MDAC should either install the patch, disable MDAC and/or RDS, or upgrade to MDAC 2.7, which is not affected by the vulnerability.
- Web client users who are running an affected version of MDAC should install the patch immediately on any system that is used for web browsing. It is important to stress that the latter guidance applies to any system used for web browsing, regardless of any other protective measures that have already been taken. For instance, a web server on which RDS had been disabled would still need the patch if it was occasionally used as a web client.

Before deploying the patch, customers should familiarize themselves with the caveats discussed in the FAQ and in the Caveats section below.

Mitigating factors:

