

Alert: Microsoft Security Bulletin MS04-003 – Buffer Overrun in MDAC Function Could Allow Code Execution (832483)

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2004-01/0014.html>

From: Russ (*Russ.Cooper_at_RC.ON.CA*)

Date: 01/13/04

Date: Tue, 13 Jan 2004 16:52:09 -0500

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Microsoft Security Bulletin MS04-003:
Buffer Overrun in MDAC Function Could Allow Code Execution (832483)

Bulletin URL:

<http://www.microsoft.com/technet/security/bulletin/MS04-003.asp>

Summary:

Version Number: V1.0

Revision Date: 01-13-2004

Impact of Vulnerability: Remote code execution

Maximum Severity Rating: Important

Patch(es) Replaced: This update replaces the one that is provided in
Microsoft Security Bulletin MS03-033.

Caveats: None

CVE Number(s): CAN-2003-0903

Tested Software:

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.ntbugtraq.com/link/39472EE8-C14A-47B4-BFCC-87988E062D91.asp>>

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

<<http://www.ntbugtraq.com/link/1D93D9E4-2B22-4595-B8C5-643824857EC0.asp>>

Software Not Affected:

Alert: Microsoft Security Bulletin MS04-003 – Buffer Overrun in MDAC Function Could Allow Code Execution

Technical Description:

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 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. Also, Microsoft Knowledge Base article 231943 discusses the release history of the different versions of MDAC.

This email is sent to NTBugtraq automatically as a service to my subscribers. (v2.3)

Cheers,

Russ – Surgeon General of TruSecure Corporation/NTBugtraq Editor

Editor's Note: The 43rd Most Powerful Person in Networking says...

Wondering how to unsubscribe from NTBugtraq? Just send a message to Listserv@listserv.ntbugtraq.com with unsubscribe ntbugtraq in the message body, you don't need a subject line. If it says you aren't subscribed, you've either subscribed with a different email address or your address has changed somehow. Just email Russ.Cooper@rc.on.ca and I'll remove you.
