

Alert: Microsoft Security Bulletin – MS02–040

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-08/0000.html>

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

Date: 07/31/02

Date: Wed, 31 Jul 2002 17:26:07 -0400

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

To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

<http://www.microsoft.com/technet/security/bulletin/MS02-040.asp>

Unchecked Buffer in MDAC Function Could Enable SQL Server Compromise (Q326573)

Originally posted: July 31, 2002

Summary

Who should read this bulletin: Database administrators using Microsoft® SQL Server(tm) 7.0 or 2000.

Impact of vulnerability: Run code of the attacker's choice.

Maximum Severity Rating: Moderate

Recommendation: Database administrators should consider installing the patch.

Affected Software:

- Microsoft Data Access Components 2.5
- Microsoft Data Access Components 2.6
- Microsoft Data Access Components 2.7

Technical description:

The Microsoft Data Access Components (MDAC) provide a number of supporting technologies for accessing and using databases. Included among these functions is the underlying support for the T-SQL OpenRowSet command. A security vulnerability results because the MDAC functions underlying OpenRowSet contain an unchecked buffer.

An attacker who submitted a database query containing a specially malformed parameter within a call to OpenRowSet could overrun the buffer, either for the purpose of causing the SQL Server to fail or causing the SQL Server service to take actions dictated by the attacker.

Mitigating factors:

- In order to exploit the vulnerability, the attacker would need the ability to load and execute a database query on the server. This is strongly discouraged by best practices, and servers that have been configured to prevent this (e.g., through the use of the DisallowAdhocAccess registry setting, as discussed in the FAQ) would not be

NT-Bugtraq: Alert: Microsoft Security Bulletin – MS02-040

at risk from the vulnerability.

- Under default conditions, the system-level privileges gained through a successful attack would be those of a Domain User.
- Even though MDAC ships as part of all versions of Windows, the vulnerability can only be exploited on SQL Servers. Customers who are not using SQL Server do not need to take action, despite the fact that MDAC may be installed on their systems.

Vulnerability identifier: CVE-CAN-2002-0695

This email is sent to NTBugtraq automatically as a service to my subscribers. Since its programmatically created, and since its been a long time since anyone paid actual money for my programming skills, it may or may not look that good...;-]

I can only hope that the information it does contain can be read well enough to serve its purpose.

Cheers,

Russ – Surgeon General of TruSecure Corporation/NTBugtraq Editor

- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)