Global Information Assurance Certification Paper

Vulnerability in Microsoft Data Access Components (MDAC) for Internet Information Server (IIS)

Kirk Cheney

April 18, 2000

Introduction

This paper is written to fulfill the Internet Research Project component of the GIAC LevelOne training course from the SANS Institute. It describes a vulnerability in Microsoft's Internet Information Server (IIS), commonly used to host Web servers, when installed with the Remote Data Service (RDS), a component of Microsoft Data Access Components (MDAC). Although first reported by Microsoft as long ago as April 22, 1998, this vulnerability continues to affect Web servers hosted using IIS.

Vulnerable systems are exposed to the risk of intruders gaining unauthorised access to the server, where they my execute shell commands, tunnel database requests to private back-end networks, or gain access to secured, non-published files on the IIS system.

This paper describes which systems are vulnerable to attack, identifies the cause of the vulnerability and presents the steps necessary to reduce or remove the risk to systems.

Affected Systems

This vulnerability affects the Remote Data Service (RDS), a component of MDAC, when installed on a system running IIS 3.0 or 4.0.

MDAC 1.5 and 2.0 are affected, as is MDAC 2.1 if installed as an upgrade from a previous version. All versions of MDAC are affected if Sample Pages for RDS are installed. The installed version of MDAC can be determined by checking the version numbers on specific DLL files. For details of these version numbers, check: http://www.microsoft.com/technet/security/bulletin/fq99-025.asp

IIS and MDAC 1.5 are installed by default as part of the Windows NT 4.0 Option Pack.

Sample Pages for RDS are available on the Windows NT 4.0 Option Pack, and the MDAC 2.0 Software Development Kit. They are installed by default in the latter.

Background

This vulnerability was first documented in Microsoft Knowledge Base article Q184375, on April 22, 1998, and later reported in Microsoft Security Bulletin (MS98-004) in July 1998. After some discussion of attack methods in Internet mailing lists, Microsoft re-released the advisory as Microsoft Security Bulletin (MS99-025) in July 1999, to remind customers of the need to address the vulnerability. However, reports of compromises continued, and on December 10, 1999, the CERT Coordination Center released CERT Incident Note IN-99-08, advising of the vulnerability and referencing these earlier bulletins.

The vulnerability arises through use of a feature in the software, and as such is not addressed by a Microsoft hot-fix, patch or service pack. The system administrator must make configuration changes to the system to reduce or remove the vulnerability, and consequently many administrators remain unaware of the issues, and many sites remain vulnerable to this attack.

For example, as recently as January 2000 the author has been involved with a site which was compromised through this vulnerability. In the early hours of New Year's Day an attacker gained access to the site's server, and replaced the organisation's home page. The server had all the current service packs and hot-fixes applied, and the site was protected by a firewall. The administrators were unaware of this vulnerability, however, and had taken no action to eliminate it, and the firewall was unable to distinguish this attack from normal Internet traffic. Fortunately, the administrators were monitoring the system for the effects of the Y2K rollover at the time, and were able to immediately rebuild the site from backups.

Description

This vulnerability lies in two components of the Remote Data Service, the DataFactory object and the VbBusObj object. The Remote Data Service is designed to enable Web clients to issue client-based SQL queries to remote data resources hosted on the IIS Web server, using *http*. The remote client communicates with the DLL, msadcs.dll, on the server, which uses the DataFactory object to enable the exchange with the database.

The problem comes about because of a feature of Microsoft's Jet database engine, which allows SQL query strings to contain additional embedded arguments, which may include VBA (Visual Basic for Applications) commands. This provides an attacker with the opportunity to execute arbitrary commands through an NT command shell, assisted by a flaw in IIS which allows ODBC commands to run with *system_local* privileges. This vulnerability was documented by Matthew Astley and rain.forest.puppy in a submission to the BugTraq mailing list, on May 25th, 1999.

The result is that the attacker can connect to a vulnerable IIS Web server across the Internet, initiate a SQL connection to a database on the server through msadcs.dll, and then issue an embedded VBA command to the server. The VBA command will be executed by the database engine, through a command shell, giving the attacker unauthorised privileged access to that server.

In the case of the DataFactory object, the attack relies on the presence of the vulnerable MDAC components, which are installed by default when IIS is installed from the Windows NT 4.0 Option Pack, and a valid Data Source Name (DSN) on the server. The DSN provides connection information for accessing the data files and specifying driver and file locations. The attacker can either use an existing DSN, or can manually specify the location of a .mdb file on the server. Therefore, any default .mdb file or DSN on the vulnerable server may be used to launch the attack. Some such files may be installed as sample files from the Windows NT 4.0 Option Pack, and others will be installed by common server applications such as Cold Fusion or iHTML; the attacker simply has to try a few default locations.

An alternative method of attack targets the VbBusObj object. This object is installed as part of the sample pages, which are available on the Option Pack, but are not installed by default. They are, however, installed by default by the MDAC 2.0 Software Developers Kit. This attack works in the same way as the DataFactory attack, with the exception that it bypasses one of the fixes available for the DataFactory vulnerability; the use of custom handlers to control or filter incoming requests. See the section below entitled "Countermeasures" for more details on custom handlers.

Detection

It should be noted that these attacks take place across an *http* session between a Web client and a Web server, using TCP port 80. Most firewalls will allow the attack to take place, as the firewall will be configured to allow Web traffic through to the Web server, and the firewall's logs will show it as normal *http* traffic.

An attack launched by exploiting this vulnerability may be detected by inspecting the IIS log files for POST access to the file /msadc/msadcs.dll. For example:

2000-01-01 02:47:39 - W3SVC1 POST /msadc/msadcs.dll - 200 0 1405 753 HTTP/1.1 ACTIVEDATA - -

However, these POST entries may be legitimate, if RDS is in use on the system.

Countermeasures

This vulnerability is not addressed by any service packs or patches. Configuration changes are required to eliminate the vulnerability.

The following configuration changes require changes to the Windows NT registry. It is recommended that these changes only be performed by an experienced administrator.

If RDS functionality is not required on your system, the following changes to the configuration of the IIS server are recommended:

1. Using the Registry editor (regedt32.exe), delete the following keys: (lines broken for clarity)
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \W3SVC\Parameters\ADCLaunch\RDSServer.DataFactory
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \W3SVC\Parameters\ADCLaunch\AdvancedDataFactory
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls

2. Delete the /msadc virtual directory and all subdirectories.

Step 1 removes the Registry entries that make the RDS objects available to the system, and step 2 removes all the files used by RDS, including msadcs.dll and all the sample files (if they were installed).

If RDS functionality is required on your system, the following changes to the configuration of the IIS server are recommended:

1. If you are running MDAC 1.5, install 2.1. From MDAC 2.0 onwards, it is possible to enable custom handlers, which enables incoming requests to be filtered. Custom handlers are enabled by setting the following registry key, using the Registry editor (regedt32.exe): (line broken for clarity)
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\DataFactory \HandlerInfo\HandlerRequired = 1 (DWORD)
2. To allow filtering of incoming requests, create a custom handler. Information on how to do this is available at: http://www.microsoft.com/Data/ado/rds/custhand.htm
3. Note that the VbBusObj object vulnerability is not affected by the above changes, as VbBusObj does not use handlers. To remove this vulnerability, delete the Registry key: (line broken for clarity)
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services \W3SVC\Parameters\ADCLaunch\VbBusObj.VbBusObjCls
4. Delete the %systemdrive%\program files\common files\system\msadc\samples directory and all subdirectories.

Steps 1 and 2 provide a means of controlling access to the RDS functions for the DataFactory object, step 3 removes the Registry entry for the VbBusObj object, making it unavailable to the system, and step 4 removes all the sample files from the server. The sample files are not designed to be available to a production server, and are not required for operation.

Summary

This paper has described a vulnerability in one of the features provided through the Remote Data Service of Microsoft's Internet Information Server, which exposes the server to the risk of compromise by a malicious attacker, across the Internet. Such an attack is capable of bypassing many firewalls.

A description of the attack method has been given, and readers have been presented with a method of identifying such an attack through subsequent analysis of the IIS log files.

Some production IIS Web Servers will have a requirement for the functionality provided by RDS, but many will not, yet still have the vulnerable services installed. This paper has presented countermeasures which will enable a system administrator to eliminate this vulnerability from their systems, whether these services are required or not.

References

The following are cited as references for this paper (in chronological order):

Bath, Kamaljit. Using the Customization Handler Feature in RDS 2.0. April 1998. http://www.microsoft.com/Data/ado/rds/custhand.htm (April 7, 2000)

Microsoft Corporation. Unauthorized ODBC Data Access with RDS and IIS. Microsoft Security Program: Microsoft Security Bulletin (MS98-004). July 17, 1998. http://www.microsoft.com/technet/security/bulletin/ms98-004.asp (April 7, 2000)

Internet Security Systems. X-Force Database Results: nt-iis-rds. August, 1998. http://xforce.iss.net/static/temp/1212.php3 (April 7, 2000)

Astley, Matthew and rain.forest.puppy. Advisory: NT ODBC Remote Compromise. BugTraq mailing list archives. May 25, 1999. http://www.securityportal.com/list-archive/bugtraq/1999/May/0216.html (April 7, 2000)

Gonzalez, Greg. FW: RDS Exploit. Windows NTBugTraq Mailing List archives. July 16, 1999.

http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind9907&L=ntbugtraq&F=P&S=&P=6565 (April 7, 2000)

Microsoft Corporation. Re-Release: Unauthorized Access to IIS Servers through ODBC Data Access with RDS. Microsoft Security Program: Microsoft Security Bulletin (MS99-025). July 19, 1999 (Revised: July 23, 1999). http://www.microsoft.com/technet/security/bulletin/ms99-025.asp (April 7, 2000)

rain.forest.puppy. Alert: IIS RDS vulnerability and fix.
Windows NTBugTraq Mailing List archives. July 23, 1999.
http://ntbugtraq.ntadvice.com/default.asp?pid=36&sid=1&A2=ind9907&L=ntbugtraq&F=&S=&P=8667 (April 5, 2000)

Cooper, Russ. IIS RDS Vulnerability. Windows NTBugTraq. July 24, 1999.
http://ntbugtraq.ntadvice.com/default.asp?sid=1&pid=47&aid=47 (April 7, 2000)

CERT Coordination Center. CERT Incident Note IN-99-08. December 10, 1999.
http://www.cert.org/incident_notes/IN-99-08.html (April 7, 2000)

Microsoft Corporation. Microsoft Security Program: Frequently Asked Questions: Microsoft Security Bulletin (MS99-025). January 4, 2000.
http://www.microsoft.com/technet/security/bulletin/fq99-025.asp (April 7, 2000)

Microsoft Corporation. PRB: Security Implications of RDS 1.5, IIS 3.0 or 4.0, and ODBC. Microsoft Product Support Services. Article ID: Q184375. February 22, 2000
http://support.microsoft.com/support/kb/articles/q184/3/75.asp (April 7, 2000)

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event