NIPC ADVISORY 99-027

"Remote Database Services Vulnerability (RDS)"

November 29, 1999

1. RDS is a known vulnerability that affects Microsoft Windows NT 4.0 servers running Internet Information Server (IIS) 3.0 and 4.0, which allows a malicious remote user to use a web browser to force a Windows NT server to return information from Sequential Query Language (SQL) databases or run system commands. Although this vulnerability was first documented in July of 1998, there has been a dramatic increase in its use over the last 30 days; both government and military systems and a Microsoft site have been compromised. Attacks have originated from both foreign and domestic sites, however as with most computer intrusion events these sites are not likely the true source of the attacks.

2. RDS allows for web clients to issue client-based SQL queries to databases hosted on a web server and then have the result set back to the client. This allows a web server to deliver records to a client and allows the browser/client to manipulate the record set, which could have a serious impact on data integrity. An intruder could also use the vulnerability to issue shell commands which could be very destructive to the web server.

3. There are unconfirmed reports of the existence of two PERL scripts (MSADC.PL and/or MSADC2.PL) that can detect the RDS vulnerability. There are also indications that a Graphical User Interface (GUI) tool is in development, which will scan for Microsoft web servers and then pass the appropriate URL and commands to exploit the vulnerability.

4. The RDS Datafactory Object, is a part of the Microsoft Data Access Components (MDAC), which are installed as part of Internet Information Server 3.0 and 4.0. This vulnerability affects MDAC 1.5 and 2.0, and will affect MDAC 2.1 if installed as an upgrade from a previous version. All versions of MDAC can become vulnerable if sample pages for RDS are installed. Sample pages are installed by default as part of the MDAC 2.0 Software Development Kit (SDK). MDAC 1.5 and IIS are installed by default as part of the Windows NT 4.0 Option Pack. The sample pages are included as part of the option pack, but are not installed by default. System administrators should note that IIS can be installed as part of other products, such as Microsoft Backoffice and Microsoft site server. The MDAC components can be installed as part of Microsoft Visual C, and Microsoft Office as well.

5. A remote intruder would typically carry out the exploitation by using a web browser to issue a command that would include the IP address of the victim, an SQL account name and password, database name and an SQL query. The query results would then be sent back to the intruder through their web browser. Despite the appearance of needing a considerable amount of insider knowledge, many sites have fallen victim to this vulnerability because of poor computer security practices. Servers need to have strong SQL passwords in addition to strong system passwords.

6. Many sites use various types of ODBC/OLE drivers in addition to the RDS Components, which can increase the risk to systems. Certain ODBC drivers can potentially allow access to files that are not published as part of the ISS server, this means that virtually any database resource that can be reached from the server can be exploited. Microsoft Datashape Provider and the Microsoft Jet OLE DB Providers (installed as part of Microsoft Visual Studio 98) are OLE drivers that will allow shell commands to be executed. Remote intruders can use a web browser in conjunction with various shell commands to cause considerable damage to a system.

7. NIPC recommends that, regardless if RDS components are needed or not, all sample pages should be deleted. The most secure method is to remove all sample pages and associated .DLL files and subdirectories. To do this go to X:\PROGRAM FILES\COMMON FILES\SYSTEM\MSADC\SAMPLES and delete everything from the samples directory and below (X: being the system drive). In addition the following registry key should be removed: HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\W3SVC\PARAMETERS\ADCLAUNCH\VBBUSOBJ.VBBUSOBJCLS

8. If RDS is not needed the following steps will disable the functionality of RDS:

   - Delete the \MSADC virtual directory from the root of the web server.
   - Remove the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\W3SVC\PARA METERS\ADCLAUNCH\RDSSERVER.DATAFACTORY
   - Remove the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\W3SVC\PARA METERS\ADCLAUNCH\ADVANCEDDATAFACTORY
   - Remove the following registry key: HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\W3SVC\PARA METERS\ADCLAUNCH\VBBUSOBJ.VBBUSOBJCLS

9. If RDS is needed, upgrade MDAC to version 2.1 and then configure it to run in "safe mode." By default, MDAC is configured to run in unsafe mode, which allows users to issue privileged commands. To get MDAC to run in safe mode, change the DWORDVALUE for the following registry key to 1:
   - Default (Unsafe Mode) Value HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\DATAFACTORY\HANDLERINFO\NAMEHANDLERREQUIREDTYPEDWORDVALUE0
   - Safe Mode Value HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\DATAFACTORY\HANDLERINFO\NAMEHANDLERREQUIREDTYPEDWORDVALUE1

   To make this process easier, Microsoft has provided a .REG file to make the change automatically. The file is available from: http://www.microsoft.com/security/bulletins/ms99-025faq.asp

10. Additional steps that can be taken to improve MDAC security are to disable anonymous users from using RDS, and to disable anonymous access to the /MSADC directory. To further increase security a custom handler file can be created to filter query requests.

11. Because a RDS attack looks like normal web server operations, it is difficult to detect. To exploit the vulnerability requires a standard HTTP "POST" to the MDAC Datafactory Object. If an intruder tried to exploit this vulnerability, there should be an IIS log entry for a "POST" to the \MSADC\MSADC.DLL file. The Datafactory Object is a standard interface, which could be used as part of a custom-built web application, but is not normally used. Unless a web server is running a custom application that calls the Datafactory Object, there will not be any IIS logs for a "POST" to the \MSADC\MSADC.DLL file. Note that if an intruder has exploited this vulnerability and has achieved privileged access, it is possible to alter IIS logs.

12. There are unconfirmed reports that there are PERL scripts that can detect the RDS vulnerability. There are also indications that a Graphical User Interface (GUI) tool is in development, that will scan for Microsoft web servers and then pass the appropriate URL and commands to exploit the vulnerability.

13. Microsoft security bulletins on this vulnerability are located at:

   - http://www.microsoft.com/security/bulletins/ms98-004.asp
   - http://www.microsoft.com/security/bulletins/ms99-025.asp

   A Microsoft knowledge base article on security implications of RDS 1.5, IIS 3.0 or 4.0, and ODBC is located at:

   - http://support.microsoft.com/support/kb/articles/q184/3/75.asp

   A Microsoft Internet Information Server 4.0 security checklist is located at:

   - http://www.microsoft.com/security/products/iis/checklist.asp

14. Recipients are asked to report significant and/or criminal activity to their local FBI office and NIPC Watch and Warning Unit, and computer emergency response support and other law enforcement agencies, as appropriate. The NIPC Watch and Warning Unit can be reached at (202) 323-3204/3205/3206, or nipc.watch@fbi.gov, with full 24 hour coverage.