

[VulnWatch] Foundstone Advisory

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2002-11/0033.html>

From: Steve W. Manzuik (steve@entrenchtech.com)

Date: 11/21/02

From: "Steve W. Manzuik" <steve@entrenchtech.com>
To: <vulnwatch@vulnwatch.org>
Date: Thu, 21 Nov 2002 11:05:11 +0900

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

Didn't see this hit the lists.

- From <http://www.foundstone.com/knowledge/randd-advisories-display.html?id=337>

Foundstone Research Labs Advisory - 112002 - MDAC

Advisory Name: Remotely Exploitable Buffer Overflow in Microsoft MDAC

Release Date: November 20, 2002

Application: MDAC versions 2.1, 2.5 and 2.6

Internet Explorer 6.0 Gold, 5.5 SP2, and 5.01 SP3

Platforms: Windows NT/2000

Severity: Critical

Vuln Type: Unauthenticated Remote Code Execution

Vendors: Microsoft Corporation (<http://www.microsoft.com>)

Authors: Barnaby Jack (labs@foundstone.com)

CVE Candidate: CAN-2002-1142

Reference: <http://www.foundstone.com/advisories>

Overview:

Microsoft Data Access Components (MDAC) is a collection of components that provide the back-end technology which enables database access for Windows platforms. MDAC is installed and implemented by default in Windows 2000, and within the Windows NT 4.0 option pack.

One of the components within MDAC, Remote Data Services (RDS), enables controlled Internet access to remote data resources through Internet Information Services (IIS). Such access allows users to execute files including .dll and .exe extensions, thereby providing increased site functionality. In general RDS embodies two functional technologies:

VulnWatch: [VulnWatch] Foundstone Advisory

Data Space and Data Control. The technology exploited within MDAC utilizes the DataSpace object of RDS which acts as a middle layer between the local command execution and the web front end. Due to incorrect string handling within the RDS interface, it is possible for a malicious user to gain control of the remote system via overrunning a buffer.

Due to the nature of the components within MDAC and RDS, Internet Explorer (IE) is also adversely affected and may be compromised by a malicious web server even if the MDAC components are not installed on the client system. Certain versions of IE allow for crafted HTTP Response packets to overrun internal components allowing for arbitrary code to be executed on the client system.

Detailed Description:

The RDS interface is provided through the file msadcs.dll. To exploit this vulnerability a user would send an IIS server a POST request to msadcs.dll and supply an abnormally long string for the Content-Type parameter; it would then overwrite various portions of heap memory. By overwriting certain function pointers within memory (eg: unhandledexceptionfilter), it is possible to kill the current thread of IIS or even execute arbitrary code within the remote process before terminating the thread.

In addition to the server-side aspect, the vulnerability also affects the RDS DataSpace object for string handling responses within Internet Explorer and may be used to exploit clients via a malicious web server. If a user were to browse a malicious site, the malicious web server could craft a remote call to force a new session that would bring the client back to the website via the new session. At this point, the server's malformed and malicious HTTP response would cause a buffer overrun within IE that could allow for the server to run unauthenticated arbitrary code on the client system before killing the IE thread.

Vendor Response:

Microsoft has released a fix for these vulnerabilities which modifies the string handling code within the DataSpace object of RDS. The fix is available at: <http://windowsupdate.microsoft.com>

Foundstone would like to thank Microsoft Security Response Center for their prompt handling of this vulnerability.

Solution:

Foundstone recommends reviewing the Microsoft Security Bulletin and immediately applying the Microsoft patch. The Microsoft Security Bulletin can be viewed at the following location.
<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q329414>

VulnWatch: [VulnWatch] Foundstone Advisory

The FoundScan Enterprise Vulnerability Management System has been updated to check for this vulnerability. For more information on FoundScan, go to: <http://www.foundstone.com>

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.0 (Build 294) Beta

iQA/AwUBPdw/VmWolZy6IFPhEQL5zwCfeQy7IzJpfVbuLMbzIYbGHG6mRvkAoLVD
Xb+kSz19BB1kk8QpNf9eNpab
=7OJ8

-----END PGP SIGNATURE-----