

CERT Advisory CA-2002-33 Heap Overflow Vulnerability in Microsoft Data

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2002-11/0003.html>

From: CERT Advisory (cert-advisory@cert.org)

Date: 11/21/02

Date: Thu, 21 Nov 2002 16:28:52 -0500

From: CERT Advisory <cert-advisory@cert.org>

To: cert-advisory@cert.org

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

CERT Advisory CA-2002-33 Heap Overflow Vulnerability in Microsoft Data
Access Components (MDAC)

Original release date: November 21, 2002

Last revised: --

Source: CERT/CC

A complete revision history can be found at the end of this file.

Systems Affected

All Microsoft Windows systems running the following:

- * Versions of Microsoft Data Access Components (MDAC) prior to 2.7
- * Internet Explorer version 6
- * Internet Explorer version 5.5
- * Internet Explorer version 5.1

Note that Microsoft Windows XP is shipped with MDAC version 2.7 and is not vulnerable by default even though Internet Explorer 6.0 is installed.

Because the normal operation of several applications and web servers on a system depend on the proper operation of the MDAC ActiveX control, other programs could be used as an exploit vector. For example, Internet Information Server may be configured to use MDAC.

Overview

A vulnerability in the Microsoft Data Access Components (MDAC) could lead to remote execution of code with the privileges of the current process or user.

I. Description

Microsoft Data Access Components (MDAC) is a collection of utilities and routines to process requests between databases and network applications. A buffer overflow vulnerability exists in the Remote Data Services (RDS) component of MDAC.

The RDS component provides an intermediary step for a client's request for service from a back-end database that enables the web site to apply business logic to the request.

According to Microsoft's Security Bulletin MS02-065, a routine in the RDS component, specifically the RDS Data Stub function, contains an unchecked buffer. The RDS Data Stub function's purpose is to parse incoming HTTP requests and generate RDS commands. This unchecked buffer could be exploited to cause a heap overflow.

There are two ways in which this vulnerability can be exploited. The first involves an attacker sending a malicious HTTP request to a vulnerable service, such as an IIS server. If RDS is enabled, the attacker can execute arbitrary code as the IIS server. RDS is not enabled by default on Windows 2000 and Windows XP systems. It can be disabled on other systems by following the advice in Microsoft's security bulletin.

The other way to exploit this vulnerability involves a malicious web site hosting a page that exploits the buffer overflow in the MDAC RDS stub through a client application, such as Internet Explorer. Most systems running Internet Explorer on operating systems other than Windows XP are vulnerable to this attack. The attacker is able to run arbitrary code as the user viewing the malicious web page.

Both web servers and client applications that rely on MDAC are affected. It is recommended that all users of Microsoft Windows 98, Windows 98 SE, Windows ME, Windows NT 4.0, and Windows 2000 apply the patch (Q329414). Windows XP users are not affected since MDAC 2.7, the non-vulnerable version, is installed by default.

Information about this vulnerability is discussed in VU#542081. This issue is also being referenced as CAN-2002-1142.

II. Impact

A remote attacker could execute arbitrary code with the privileges of the application that processed the request.

In the case of a web server or other service, this is likely to be the SYSTEM or another account with elevated privileges. In the case of a client application, this will be the account used to view the web page.

III. Solution

Apply a patch from your vendor.

Microsoft has released a patch (Q329414) and a security bulletin (MS02-065) to address this issue. An end-user version of MS02-065 is available at

http://www.microsoft.com/security/security_bulletins/ms02-065.asp.

According to the Microsoft advisory, a scenario exists in by which a vulnerable version of the control may be re-installed on a Windows system even after the patch has been applied. This is due to the fact that the vulnerable ActiveX control is signed by Microsoft and the patch does not set the kill bit for the MDAC control.

This vulnerability was reported in an advisory by Foundstone and in MS02-065 by Microsoft.

Feedback can be sent to the Authors: Jason A. Rafail, Chad R. Dougherty, and Cory F. Cohen.

This document is available from:

<http://www.cert.org/advisories/CA-2002-33.html>

CERT/CC Contact Information

Email: cert@cert.org

Phone: +1 412-268-7090 (24-hour hotline)

Fax: +1 412-268-6989

Postal address:

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh PA 15213-3890
U.S.A.

CERT/CC personnel answer the hotline 08:00-17:00 EST(GMT-5) / EDT(GMT-4) Monday through Friday; they are on call for emergencies during other hours, on U.S. holidays, and on weekends.

Using encryption

We strongly urge you to encrypt sensitive information sent by email.

Our public PGP key is available from

http://www.cert.org/CERT_PGP.key

Cert: CERT Advisory CA-2002-33 Heap Overflow Vulnerability in Microsoft Data

If you prefer to use DES, please call the CERT hotline for more information.

Getting security information

CERT publications and other security information are available from our web site

<http://www.cert.org/>

To subscribe to the CERT mailing list for advisories and bulletins, send email to majordomo@cert.org. Please include in the body of your message

subscribe cert-advisory

* "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office.

NO WARRANTY

Any material furnished by Carnegie Mellon University and the Software Engineering Institute is furnished on an "as is" basis. Carnegie Mellon University makes no warranties of any kind, either expressed or implied as to any matter including, but not limited to, warranty of fitness for a particular purpose or merchantability, exclusivity or results obtained from use of the material. Carnegie Mellon University does not make any warranty of any kind with respect to freedom from patent, trademark, or copyright infringement.

Conditions for use, disclaimers, and sponsorship information

Copyright 2002 Carnegie Mellon University.

Revision History

November 21, 2002: Initial release

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

Version: PGP 6.5.8

```
iQCVAwUBPd1NYGjtSoHZUTs5AQHUzAQAx1VWaNhv/9ihPvBWXPUNmrQxcF3AGx
SCtW1Lsgs7b0LHeNFKwEYxQu7nBGoc4otgQ1oVj+ftJwOHSA560qPB9Pbu7doSG
7Hql8T/LdOGgcRIAPmLPvAK1rDT2oN85S/adpaQgFRgQw7RYLMsgjCKmQivpCpDA
/8Vb+bI52YU=
```

=3mho

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