

CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

Source: <http://www.derkeiler.com/Mailing-Lists/Cert/2002-02/0002.html>

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

Date: 02/25/02

Date: Mon, 25 Feb 2002 11:57:58 -0500 (EST)

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

To: cert-advisory@cert.org

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

CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

Original release date: February 25, 2002

Last revised: --

Source: CERT/CC

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

Systems Affected

- * Microsoft Internet Explorer
- * Microsoft Outlook and Outlook Express
- * Other applications that use the Internet Explorer HTML rendering engine

Overview

Microsoft Internet Explorer contains a buffer overflow vulnerability in its handling of embedded objects in HTML documents. This vulnerability could allow an attacker to execute arbitrary code on the victim's system when the victim visits a web page or views an HTML email message.

I. Description

Internet Explorer supports the <EMBED> directive, which can be used to include arbitrary objects in HTML documents. Common types of embedded objects include multimedia files, Java applets, and ActiveX controls. The SRC attribute specifies the source path and filename of an object. For example, a MIDI sound might be embedded in a web page with the following HTML code:

```
<EMBED TYPE="audio/midi" SRC="/path/sound.mid" AUTOSTART="true">
```

Internet Explorer uses attributes of the <EMBED> directive and MIME information from the web server to determine how to handle an embedded object. In most cases, a separate application or plugin is used.

A group of Russian researchers, SECURITY.NNOV, has reported that Internet Explorer does not properly handle the SRC attribute of the <EMBED> directive. An HTML document, such as a web page or HTML email message, that contains a crafted SRC attribute can trigger a buffer overflow, executing code with the privileges of the user viewing the document. Microsoft Internet Explorer, Outlook, and Outlook Express are vulnerable. Other applications that use the Internet Explorer HTML rendering engine, such as Windows compiled HTML help (.chm) files and third-party email clients, may also be vulnerable.

The CERT/CC is tracking this vulnerability as VU#932283, which corresponds directly to the "buffer overrun" vulnerability described in Microsoft Security Bulletin MS02-005.

This vulnerability has been assigned the CVE identifier CAN-2002-0022.

II. Impact

By convincing a user to view a malicious HTML document, an attacker can cause the Internet Explorer HTML rendering engine to execute arbitrary code with the privileges of the user who viewed the HTML document. This vulnerability could be exploited to distribute viruses, worms, or other malicious code.

III. Solution

Apply a patch

Microsoft has released a cumulative patch for Internet Explorer that corrects this vulnerability and several others. For more information about the patch and the vulnerabilities, please see Microsoft Security Bulletin MS02-005:

<http://www.microsoft.com/technet/security/bulletin/MS02-005.asp>

Disable ActiveX Controls and Plugins

In Internet Explorer, plugins may be used to view, play, or otherwise process embedded objects. The execution of embedded objects is controlled by the "Run ActiveX Controls and Plugins" security option. Disabling this option will prevent embedded objects from being processed, and will therefore prevent exploitation of this vulnerability.

According to MS02-005:

Cert: CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

The vulnerability could not be exploited if the "Run ActiveX Controls and Plugins" security option were disabled in the Security Zone in which the page was rendered. This is the default condition in the Restricted Sites Zone, and can be disabled manually in any other Zone.

At a minimum, disable the "Run ActiveX Controls and Plugins" security option in the Internet Zone and the zone used by Outlook or Outlook Express. The "Run ActiveX Controls and Plugins" security option is disabled in the "High" zone security setting. Instructions for configuring the Internet Zone to use the "High" zone security setting can be found in the CERT/CC Malicious Web Scripts FAQ:

http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

Apply the Outlook Email Security Update

Another way to effectively disable the processing of ActiveX controls and plugins in Outlook is to install the Outlook Email Security Update. The update configures Outlook to open email messages in the Restricted Sites Zone, where the "Run ActiveX Controls and Plugins" security option is disabled by default. In addition, the update provides further protection against malicious code that attempts to propagate via Outlook.

- * Outlook 2002 and Outlook Express 6

The functionality of the Outlook Email Security Update is included in Outlook 2002 and Outlook Express 6.

- * Outlook 2000

<http://office.microsoft.com/downloads/2000/Out2ksec.aspx>

- * Outlook 98

<http://office.microsoft.com/downloads/9798/Out98sec.aspx>

Appendix A. – Vendor Information

This appendix contains information provided by vendors for this advisory. When vendors report new information to the CERT/CC, we update this section and note the changes in our revision history. If a particular vendor is not listed below, we have not received their comments.

Microsoft

Microsoft has released a Security Bulletin and a Knowledge Base Article addressing this vulnerability:

- * Security Bulletin MS02-005

<http://www.microsoft.com/technet/security/bulletin/MS02-005.asp>

- * Knowledge Base Article Q317731

<http://support.microsoft.com/default.aspx?scid=kb:en-us:Q317731>

Cyrusoft

Cert: CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

Our email client Mulberry does not use the core HTML rendering engine library for its HTML display, and so is not affected by the bug in that library. Having looked at the details of this alert I can also confirm that our own HTML rendering engine is not affected by this, as it ignores the relevant tags.

Appendix B. – References

1. <http://www.kb.cert.org/vuls/id/932283>
2. <http://www.security.nnov.ru/advisories/mshtml.asp>
3. <http://www.microsoft.com/technet/security/bulletin/MS02-005.asp>
4. <http://support.microsoft.com/default.aspx?scid=kb:en-us:Q317731>
5. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0022>
6. <http://msdn.microsoft.com/workshop/author/dhtml/reference/objects/embed.asp>
7. <http://developer.netscape.com/docs/manuals/htmlguid/tags14.htm#1286379>

The CERT/CC thanks ERRor and DarkZorro of domain Hell and 3APA3A of SECURITY.NNOV for reporting this issue to us.

Author: Art Manion

This document is available from:
<http://www.cert.org/advisories/CA-2002-04.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

Cert: CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

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

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

February 25, 2002: Initial release

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

Version: PGP 6.5.8

iQCVAwUBPHppRKCVPmXQI2HJAQEunQP9Hn+YSjmwNSLM4//5JrHP0ydgT0DFzh5k
0X40VYjxXcls0r3uZrpfC80W2f7DF3IS2kNcys4aEl+OXkTLn3p2BEkGYFhitwbG
Tl0KvoESvT6b/1/w3TCjBregrAxPEXdw9KwQ2JFm/jmpX1+Gr15X7b2TDbf4sxJy
q3UC1EPU9JE=
=Jtq3

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

Cert: CERT Advisory CA-2002-04 Buffer Overflow in Microsoft Internet Explorer

- ***Previous message:*** CERT Advisory: "CERT Advisory CA-2002-03 Multiple Vulnerabilities in Many Implementations"
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]