

How Outlook 2002 can still execute JavaScript in an HTML email message

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2002-03/0037.html>

From: Richard M. Smith (rms@COMPUTERBYTESMAN.COM)

Date: 03/21/02

Date: Thu, 21 Mar 2002 14:55:53 -0500
From: "Richard M. Smith" <rms@COMPUTERBYTESMAN.COM>
To: NTBUGTRAO@LISTSERV.NTBUGTRAO.COM

Hello,

Windows Media Player (WMP) reintroduces the ability to automatically execute JavaScript code from an HTML email message in Outlook 2002. JavaScript is disabled by default in Outlook 2002, because it can facilitate the creation of worms and other malicious code which is carried by HTML email messages. Using a number of simple tricks, WMP can be used to bypass the Outlook security settings and still automatically execute JavaScript, Java, and ActiveX code in an HTML email message.

Here is an outline of the steps needed to exploit this problem:

1. An IFRAME tag is inserted into an HTML email message that references a Windows Media Skin (.WMS) file. The .WMS can be loaded either from a Web site or from an attached file to the email message using the CID: protocol. (Note: I have only tested downloading a .WMS file from a Web site.)
2. Because .WMS files are considered safe by Windows, WMP will automatically be started by Outlook and it will be passed the .WMS file.
3. The .WMS file contains a short bit of JavaScript code in an onload handler which runs a Web page using the player.LaunchURL() method. This onload handler is automatically executed when WMP opens the .WMS file.
4. The Web page from step 3 can be loaded from a Web site, or the source code of the Web page can be embedded in the .WMS file using the "about:" or "javascript:" protocol.

Notes

NT–Bugtraq: How Outlook 2002 can still execute JavaScript in an HTML email message

1. Other WMP file types besides a Windows Media skin file can be used in step 1. These file types include .WMZ, .WMD, and .WMA files.
2. This problem is more of an example of poor security policies in Outlook and WMP and is not really a security hole in the classic sense.
3. Outlook Express and earlier versions of Outlook likely have the same security problem even with all security protections set to the maximum.
4. Hotmail however does not seem to have this security problem because it discards IFRAME tags. Other Web–based email systems however would have the same security problem as Outlook if they do not do filtering of IFRAMEs.

Recommendations

1. Outlook 2002 should not execute files downloaded by an HTML IFRAME tag. All file types except for HTML, text, and image files should be discarded by Outlook 2002 if used in an IFRAME.
2. All WMP file types (.ASX, .WMS, .WMZ, .WMD, .WMA, etc.) should not be marked safe for opening since many of them can contain script code.
3. The "about:" and "javascript:" protocols should be disabled in the player.LaunchURL() method.

Workarounds

The only work–around that I am aware of is to manually mark each Windows Media file type as not safe–for–opening. This process is going to be prone to errors since there are about 10 file types that need to be fixed.

Richard M. Smith
<http://www.ComputerBytesMan.com>

-
- ***Previous message:*** [Michel Arboi: "Re: Potential vulnerabilities of the Microsoft RVP–based Instant Messaging"](#)
 - ***Next in thread:*** [Agricola: "Re: How Outlook 2002 can still execute JavaScript in an HTML email message"](#)
 - ***Reply:*** [Agricola: "Re: How Outlook 2002 can still execute JavaScript in an HTML email message"](#)
 - ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)