

EEYE: Internet Explorer Object Data Remote Execution Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-08/0101.html>

From: Marc Maiffret (marc_at_EEYE.COM)

Date: 08/21/03

Date: Thu, 21 Aug 2003 11:56:36 -0700

To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

The first time I sent this email it included example HTML code. That HTML code would have no affect on eMail clients as this is not a HTML email nor was the data properly formatted, etc..., etc... However, due to VERY POORLY written mail gateways, this eMail was being blocked at most gateways as being a virus etc... Hence I have removed that data (you can find it on the eEye website) and I am resending the advisory. So no need to eMail me about this, I am aware of all those using poorly written software to protect their organization, McAfee Groupshield being the biggest culprit.

-Marc

Internet Explorer Object Data Remote Execution Vulnerability

Release Date:

August 20, 2003

Reported Date:

May 15, 2003

Severity:

High (Remote Code Execution)

Systems Affected:

Microsoft Internet Explorer 5.01

Microsoft Internet Explorer 5.5

Microsoft Internet Explorer 6.0

Microsoft Internet Explorer 6.0 for Windows Server 2003

Description:

eEye Digital Security has discovered a security vulnerability in Microsoft's Internet Explorer that would allow executable code to run automatically upon rendering malicious HTML.

This is a flaw in Microsoft's primary contribution to HTML, the Object tag,

NT-Bugtraq: EEYE: Internet Explorer Object Data Remote Execution Vulnerability

which is used to embed basically all ActiveX into HTML pages. The parameter that specifies the remote location of data for objects is not checked to validate the nature of the file being loaded, and therefore trojan executables may be run from within a webpage as silently and as easily as Internet Explorer parses image files or any other "safe" HTML content.

This attack may be utilized wherever IE parses HTML, including web sites, e-mail, newsgroups, and within applications utilizing web-browsing functionality.

Note:

On Windows 2003 Internet Explorer, this upgrade is noted as being "moderate" rather than "critical." This is said to be because of Windows 2003's "Enhanced Security Configuration Mode." In plain English, this just means that Microsoft checked the "Disable ActiveX" box on Internet Explorer's Security Properties. Windows 2003 Internet Explorer also disables by default Visual Basic Script, Javascript, input forms, and even the ability to download files.

Due to the popularity and prevalence of ActiveX on the Internet, users running Windows 2003 "Enhanced Security Configuration" Mode may have chosen to reactivate the ability to view active content. These users should be aware that they are at critical risk for this vulnerability and should apply the necessary patch.

Lastly, Microsoft attributes credit to eEye for this bug, stating it is the "Object Type" bug. They do this after noting a variant of the "Object Type" bug was found to be still vulnerable on certain language based systems. However, the "Object Type" bug was our previous "Object" tag vulnerability. That issue involved a stack based overflow in the "Type" property. This current issue involves incorrect handling of the data specified by the "Data" tag.

Technical Description:

[Data Removed] We have removed the example data from this eMail due to mail gateway filters not functioning properly and believing this eMail is a virus. For the full advisory with all technical details please visit: <http://www.eeye.com/html/Research/Advisories/AD20030820.html>

This example is in the more traditional vein. In house, we set up a demonstration system that silently loaded "bo2k" and "subseven" trojans from within a single webpage.

The above example shows an entirely legitimate session. The only trick to this is that the "Data" URL must not end in an unsafe extension (e.g., ".exe", ".bat", etc). The "Content-Type" tag returned by the server is treated by Internet Explorer as authoritative.

NT–Bugtraq: EEYE: Internet Explorer Object Data Remote Execution Vulnerability

In other words, the client asks for a safe file, the server returns an unsafe file, and Internet Explorer does not know what hit it.

What Internet Explorer should be doing in this case is not loading the unsafe document at all, or it should prompt the user with a severe warning about this file, with the default option being to save the file to disk.

We can generally guess what is going on here. As .hta or "HTML Application" files are not binary and resemble – mechanically – HTML files, IE's check of content will be unable to return that this file is anything but safe. The second check of MIME type will see that we are requesting a safe file type... and the third check of MIME type will be from the server saying this is a HTML Application. For whatever reason, IE has ignored the returned MIME type from a security context, but paid attention to it from an execution context.

This attack was discovered through manual testing techniques. The hypothesis was: "Internet Explorer has many avenues where it might be presented with executable content. One of these avenues must be broken so that executable content might be automatically run."

Protection:

Retina Network Security Scanner has been updated to identify this latest Internet Explorer vulnerability.

Vendor Status:

Microsoft was notified and has released a patch for this vulnerability. The patch is available at:

<http://www.microsoft.com/technet/security/bulletin/MS03-032.asp>

Credit:

Drew Copley (dcopley@eeye.com), Research Engineer, eEye Digital Security

Greetings: Liu Die Yu, http-equiv, Stone Fisk, Dror Shalev, the Shrug, Oliver Lavery, Brett Moore, Chung's Donut Shop, Jolly

Copyright (c) 1998–2003 eEye Digital Security

Permission is hereby granted for the redistribution of this alert electronically. It is not to be edited in any way without express consent of eEye. If you wish to reprint the whole or any part of this alert in any other medium excluding electronic medium, please e-mail alert@eEye.com for permission.

Disclaimer

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

