

Internet Explorer Object Type Property Overflow

Source: <http://www.derkeiler.com/Mailing-Lists/NT-Bugtraq/2003-06/0008.html>

From: Derek Soeder (*dsoeder_at_EEYE.COM*)

Date: 06/04/03

Date: Wed, 4 Jun 2003 12:00:07 -0700
To: NTBUGTRAQ@LISTSERV.NTBUGTRAQ.COM

Internet Explorer Object Type Property Overflow

Release Date:
June 4, 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:

The "Object" tag is used to insert objects such as ActiveX components into HTML pages. The "Type" property of the "Object" tag is used to set or retrieve the MIME type of the object. Typical valid MIME types include "plain/text" or "application/hta", "audio/x-mpeg", etc. A buffer overflow has been discovered in the "Type" property of the "Object" tag. While there is buffer checking in place, the buffer checking can be overcome by using a special character. From there, the exploitation is a simple, stack-based overflow that allows the remote attacker to run code of his/her choice on the target system.

This attack may be utilized wherever IE parses HTML, so this vulnerability, affects newsgroups, mailing lists, or websites.

Note:

Due to the popularity and prevalence of ActiveX on the Internet, users running Windows 2003 "Enhanced Security Configuration" Mode may have chosen to re-activate the ability to view active content for all websites instead of continually adding websites to the "Internet" or "Trusted" zones on a per-site basis. These users should be aware that they are at risk for this vulnerability and should apply the necessary patch.

Technical Description:

NT–Bugtraq: Internet Explorer Object Type Property Overflow

This example was designed for Windows 2000 with .Net Framework and the latest IE.

```
<object type="[x64]AAAAAAAAAAAAAAAA">Cooler Than Centra Spike</object>
```

Give or take a few '/' characters depending on the system. The issue is relatively simple and interesting: the '/' character is changed into '_/__' (three characters) after the string is checked for proper buffer size. Because of this expansion, we are able to overrun the bounds of the buffer. This allows us to take control of key registers so as to run code that we specify, which will be available at the EDX register. At this point a JMP EDX is called, and from there the payload can be executed.

This issue was discovered by using the same automated testing tool with which we found the Shockwave, MSN Chat, and PNG issues. Additional time was saved through "eVe", a proprietary vulnerability tracing tool which allows for the viewing of checked and unchecked buffers as they are processed in memory.

Protection:

Retina® Network Security Scanner (<http://www.eeye.com/Retina>) 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/MS03-020.asp>

Credit:

Drew Copley, Research Engineer, eEye Digital Security

Greetings:

Thanks to Riley Hassell, Research Engineer — for eVe, and various other research help. Welcome to Unyun, of ShadowPenguin fame — he swears there are no ninjas left in Japan, but he is lying, and he is one. Also gr33t5 to... the Shadow, Wolverine, the Hulk, and the Punisher.

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.

