

[VulnWatch] [EEYEB-20080824] Internet Explorer Compressed Content URL Heap Overflow Vulnerability #2

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-09/msg00007.html>

- *From:* "eEye Advisories" <Advisories@xxxxxxxx>
 - *Date:* Tue, 12 Sep 2006 15:28:12 -0700
-

Internet Explorer Compressed Content URL Heap Overflow Vulnerability #2

<http://research.eeye.com/html/advisories/published/AD20060912.html>

Release Date:

September 12, 2006

Date Reported:

August 24, 2006

Severity:

High (Code Execution)

Systems Affected:

Internet Explorer 5 SP4 with MS06-042 – Windows 2000

Internet Explorer 6 SP1 with MS06-042 v1 or v2 – Windows 2000

Internet Explorer 6 SP1 with MS06-042 v1 or v2 – Windows XP SP1

Internet Explorer 6 SP1 with MS06-042 v1 or v2 – Windows Server 2003 SP0

Overview:

eEye Digital Security has discovered a second heap overflow vulnerability in the MS06-042 cumulative Internet Explorer update that would allow an attacker to execute arbitrary code on the system of a victim who attempts to access a malicious URL. Windows 2000, Windows XP SP1, and Windows 2003 SP0 systems running Internet Explorer 5 SP4 or Internet Explorer 6 SP1, with the MS06-042 patch applied, are vulnerable; unpatched and more recent versions of Internet Explorer are not affected.

This heap overflow is almost identical to the previous vulnerability reported by eEye and addressed in the August 24th re-release ("v2") of MS06-042. In this case, the heap overflow occurs when URLMON.DLL attempts to handle a long URL for which the web server's response indicated GZIP or deflate encoding, if that URL was returned as the destination of an HTTP redirect (e.g., "302 Found"). This means that the user interaction requirement for this attack is negligible, since clicking a hyperlink, visiting a malicious web page, or even attempting to view an image for which the source is a malicious URL, permits exploitation of the vulnerability.

Technical Details:

URLMON.DLL versions 5.0.3841.2400, 6.0.2800.1565, and 6.0.2800.1567, distributed with the MS06-042 patches for Internet Explorer 5 SP4 and Internet Explorer 6 SP1 on Windows 2000, Windows XP SP1, and Windows 2003 SP0, contain a heap buffer overflow vulnerability due to an incongruous use of `IstrcpynA`. `CMimeFt::Create` allocates a 390h-byte heap block for a new instance of the `CMimeFt` class, within which there is a 104h (`MAX_PATH`)-byte ASCII string buffer at offset +160h:

```
1A4267F8 push 390h ; cb
```

```
1A4267FD call ??2@YAPAXI@Z ; operator new(uint)
```

When an access to a URL elicits an HTTP redirect (statuses 300 through 303) from the web server, and the subsequent access to the "Location" URL returns a GZIP- or deflate-encoded response, `CMimeFt::ReportProgress` will attempt to copy the URL into the 104h-byte string buffer using the `IstrcpynA` API function, but it passes a maximum length argument of 824h (2084 decimal), a value typically used as the maximum length of a URL:

```
1A425D41 push 824h ; iMaxLength
```

```
1A425D46 push eax ; lpString2
```

```
1A425D47 add esi, 15Ch
```

```
1A425D4C push esi ; lpString1
```

```
1A425D4D call ds:lstrcpynA
```

As a result, fields within the CMimeFt class instance, as well as the contents of adjacent heap blocks, can be overwritten with attacker-supplied data from the malicious URL.

Windows XP SP2 and Windows 2003 SP1 are not susceptible because the URLMON.DLLs included in the MS06-042 patches for those systems use 824h both as the field size and as the copy length limit, in all the relevant locations in the code. The QFE branches of MS06-042 even for the above-mentioned vulnerable versions of Windows and Internet Explorer are not susceptible for the same reason; it is unclear why this fix was repeatedly re-implemented, in many cases incorrectly, when proper implementations have existed since August 8th.

Protection:

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

Vendor Status:

Microsoft has released a third version of the MS06-042 patch to correct this vulnerability. The revised patch is available at:

<http://www.microsoft.com/technet/security/bulletin/MS06-042.msp>.

Note that installing the original release or first re-release of the MS06-042 update causes a system to become vulnerable, so applying the version 3.0 release of the MS06-042 patch will then be necessary in order to secure that system.

Systems with the QFE version of the MS06-042 v1 or MS06-042 v2 / KB923762 hotfix applied are not susceptible to this vulnerability, although the MS06-042 v3.0 patch should still be installed on these systems. (Note that the QFE DLL is only selected in specific, rare circumstances, so most likely applying MS06-042 v1 or v2 will deploy the vulnerable GDR-branch DLL instead.)

Credit:

Derek Soeder

Related Links:

Retina Network Security Scanner –
(<http://www.eeye.com/html/products/retina/index.html>)

Blink Endpoint Vulnerability Prevention –
(<http://www.eeye.com/html/products/blink/index.html>)

Greetings:

Eric B. for discovering and contributing the premier.microsoft.com proof-of-concept URL. 3x charm.

Copyright (c) 1998-2006 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 email alert@xxxxxxxx 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, implied or express, with regard to this information. In no event shall the author be liable for any direct or

indirect 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.