

RE: MSIE Download Window Filename + Filetype Spoofing Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2004-07/0201.html>

From: Eric McCarty (*eric_at_lawmpd.com*)

Date: 07/12/04

Date: Mon, 12 Jul 2004 13:38:56 -0700

To: "Drew Copley" <dcopley@eEye.com>, "Paul" <paul@greyhats.cjb.net>, <bugtraq@securityfocus.com>

The examples do not work on XP Sp2 version of IE. (6.0.2900.2149).

E.

-----Original Message-----

From: Drew Copley [mailto:dcopley@eEye.com]

Sent: Monday, July 12, 2004 11:21 AM

To: Paul; bugtraq@securityfocus.com

Subject: RE: MSIE Download Window Filename + Filetype Spoofing Vulnerability

This is an open bug. (One which is rather disturbing, so I am not sure why Microsoft has chosen to not fix it.)

Date: 21 October 2001

<http://www.guninski.com/popspooft.html>

"Demonstration:

Image moving over download/open dialog:

<http://www.guninski.com/opf2.html> "

> -----Original Message-----

> From: Paul [mailto:paul@greyhats.cjb.net]

> Sent: Sunday, July 11, 2004 8:52 AM

> To: bugtraq@securityfocus.com

> Subject: MSIE Download Window Filename + Filetype Spoofing

> Vulnerability

>

>

>

> Note: This vulnerability as well as several more can be found

> at <http://www.greyhats.cjb.net>

>
>
>
> *Download Window Filename + Filetype Spoofing Vulnerability*
>
>
>
> *[Tested]*
>
> *IEXPLORE.EXE file version 6.0.2800.1106*
>
> *MSHTML.DLL file version 6.00.2800.1400*
>
> *Microsoft Windows XP sp2*
>
>
>
> *[Discussion]*
>
> *When a webpage offers a file whose mime type can't be opened*
> *in a browser, Internet Explorer usually displays a download*
> *window with the filename and its type. Previous*
> *vulnerabilities have been used to spoof the filename so the*
> *victim thinks the file is something it isn't. This is one of*
> *those vulnerabilities.*
>
>
>
> *Window.createPopup() creates a popup that goes on top of*
> *every other window. This includes applications other than*
> *Internet Explorer. This doesn't seem like the greatest idea,*
> *but it could be useful if you want to get urgent information*
> *out to someone. By placing the popup in a certain location,*
> *we can cover up the filename and its type in the download*
> *window and replace it with our own. One more thing, we need*
> *to set the popup's onunload to open itself back up, because*
> *if the parent window is clicked after a popup opens, the*
> *popup is closed.*
>
>
>
> *The example tells Internet Explorer to download badfile.exe,*
> *which of course is an 'Application'. A popup is then opened*
> *covering up the filename and type and replaces it with*
> *'sexycoeds.jpg' (GGW commercial was on when I was writing*
> *this ;) which is a 'JPEG Image'. The viewer should press*
> *'open' to view the sexy coeds right away, which will download*
> *and run badfile.exe. If you want, you can name the executable*
> *sexycoeds.exe and change the icon so if the user presses*
> *'save' windows should hide the extension and it will still*
> *look like a jpg image.*

SecurityFocus Bugtraq: RE: MSIE Download Window Filename + Filetype Spoofing Vulnerability

>

>

>

> *[Example]*

>

> <http://freehost07.websamba.com/greyhats/dlwinspoof.htm>

>