

RE: Drivial Pursuit: Internet Explorer Browser & Your Files and Folders !

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2003-07/0309.html>

From: Thor Larholm (*thor_at_pivx.com*)

Date: 07/24/03

To: <bugtraq@securityfocus.com>

Date: Wed, 23 Jul 2003 17:07:26 -0700

I can positively confirm this vulnerability on both WMP 7 and 8 on Windows 98, ME, 2000, XP and 2003. The default Enhanced Security Configuration of IE on Windows 2003 does nothing to prevent automatically opening certain media types.

The ASF file can be automatically opened through an IFRAME, both on a webpage and in an email – even with scripting disabled in the Restricted Zone, which has so far been a major mitigating factor. This means that an emailborne exploit would execute immediately when a user opened or previewed an HTML-based email.

Regards

Thor Larholm

PivX Solutions, LLC – Senior Security Researcher

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

From: http-equiv@excite.com <1@malware.com>

Subject: Drivial Pursuit: Internet Explorer Browser & Your Files and Folders !

Wednesday, 23 July, 2003

Yet another quaint lead-up to "silent delivery and installation of an executable on a target computer. No client input other than viewing a web page" !

This is getting boring.

A myriad of technical hurdles have been recently placed to disallow access to files and folders on the local machine from the internet. Previously simple redirects could defeat that, but that too has been eliminated.

Coupled with a myriad of existing possibilities of placing arbitrary files in known locations on the local machine, along with perhaps

SecurityFocus Bugtraq: RE: Drivial Pursuit: Internet Explorer Browser & Your Files and Folders !

several other well known applications that create sensitive files in known locations on the local machine, accessing all of these with our trusty browser commonly known as IE, leaves us with ample opportunity to wreak further havoc on the unsuspecting customers of the manufacturer, one "Microsoft".

For an ever increasing list of component possibilities seek here:

<http://www.pivx.com/larholm/unpatched/>

Once again the problem lies within our trusty and battle-hardened Windows Media Player. Two second creation of Zero second URL flip to local machine, allows us the desired access. Whether this is the result of a 'trusted' media file or not is unclear. Not important. Custom crafted media files seem to fail.

Working Example:

Fails on WMP 9 but fully functional on all others regardless of operating system:

ATTENTION: demo is merely first step. Plug 'n Play any of the available components in the listing above for maximum results:

<http://www.malware.com/once.again!.html>

Notes:

1. We appear to be going around and around in circles now
2. We see no possibility of ever expending one red cent to this particular toy manufacturer. As such we are stuck with what we have. We would be interested to thoroughly examining the latest and greatest toys created by these people and should someone feel like lending us a couple shiny new machines with default installs of the latest and greatest toys, we'll be happy come to some sort of mutually beneficial arrangement.
3. None.

--

<http://www.malware.com>