

RE: Comments on 5 IE vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/focus-ms/2003-12/0007.html>

From: Fred Langston (Fred.Langston_at_guardent.com)

Date: 12/03/03

To: 'Thor Larholm' <thor@pivx.com>, focus-ms@securityfocus.com

Date: Tue, 2 Dec 2003 19:14:16 -0500

For those who have opened up the Internet Options, Security tab and are saying, "I don't have a My Computer Zone!", here's the solution:

<http://support.microsoft.com/?kbid=315933>

Fred Langston, CISSP

Senior Principal Consultant

W: 206.903.8147 x223 F: 206.903.1862 M: 425.765.3330

Seattle, WA www.Guardent.com

G U A R D E N T

Enterprise Security and Privacy Programs

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

From: Thor Larholm [<mailto:thor@pivx.com>]

Sent: Tuesday, December 02, 2003 11:15 AM

To: focus-ms@securityfocus.com

Subject: FW: Comments on 5 IE vulnerabilities

I thought this might be of interest to the focus-ms list as well :)

Regards

Thor Larholm

Senior Security Researcher

PivX Solutions, LLC

Get our research, join our mailinglist - <http://pivx.com/larholm/>

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

From: Thor Larholm

Sent: Monday, December 01, 2003 3:36 PM

To: bugtraq@securityfocus.com

Subject: Comments on 5 IE vulnerabilities

Despite the severity of some of the vulnerabilities posted by Liu Die Yu, such as the ability for system compromises, it is relatively easy to mitigate against the impact and even prevent them from having any effect at all.

RE: Comments on 5 IE vulnerabilities

SecurityFocus Microsoft: RE: Comments on 5 IE vulnerabilities

Much ado has been made about those vulnerabilities and they have been covered in numerous places such as Forbes, NY Times and CNN. What this tells me is that we need a radically different approach than the status quo. One such approach is to put more emphasis on education and secure coding, so that we can reliably prevent future threats. Another such approach is to focus on proactive security measures that prevent vulnerabilities and design flaws from having any effect in advance, prior to their discovery and publication. We can recognize the common pathways that these vulnerabilities rely on and act accordingly.

When I attended the NTBugtraq Retreat earlier this year, most of the attendees were surprised to hear that I am using Internet Explorer on a daily basis, particularly since I should know how vulnerable it can be at any given time. I surf with JavaScript and ActiveX enabled, see flash movies and play Java games, but despite this I am not vulnerable [0] to a single command execution vulnerability or system compromise through Internet Explorer.

How, you might ask? Simple, I have locked down the My Computer security zone on my installations [1].

Each and every command execution vulnerability in Internet Explorer over the last few years have all depended on the functionality of local security zones. Whenever you are crafting an exploit, you want to navigate a window object to a local security zone, inject some scripting or HTML into the window object and subsequently use the features of the local security zone to execute your payload. Properly locking down the My Computer zone prevents all of these from having any effect.

However, changing the Internet Explorer security zone settings is not a nimble task. Despite being partly split after IE4, the functionality of Windows Explorer and Internet Explorer is still very tightly interwoven. If you are not careful you WILL cause your system to malfunction and no longer open Explorer folders, launch applications or even boot into Windows properly. You need to strike a very sensible balance.

During the course of our research, we crafted and tested solutions to this problem on tens of thousands of installations and have beta tested on thousands of users, and have incorporated the results into our FREE constantly updated Proactive Threat Mitigation application that goes by the name of Qwik-Fix(r) (www.pivx.com/qwikfix/). Our beta users were never affected by Blaster, HTAExploit or MiMail – to name a few.

Now, let's analyze the vulnerabilities Liu Die Yu posted on November 25th [2], as there was not much details in the post.

"1stCleanRc" is not a vulnerability of its own, but an example exploit detailing how to combine the "MhtRedirParsesLocalFile", "BackToFramedJpu" and "MhtRedirLaunchInetExe" vulnerabilities. The same goes for "execdror6" which is an example exploit that relies on the "LocalZoneInCache" vulnerability, as well as "LocalZoneInCache" which is a demonstration of

SecurityFocus Microsoft: RE: Comments on 5 IE vulnerabilities

using "threadid10008".

This leaves us with 5 vulnerabilities to analyze:

MhtRedirParsesLocalFile is designed to display and parse a locally residing file of any plaintext format in an IFRAME. On most of our installations we could only reproduce the display part. Still, being able to display a locally residing file in a window object is specifically prohibited by IE6 SP1.

MhtRedirLaunchInetExe expands a bit on the capabilities of the codeBase vulnerability. Microsoft fixed codeBase in the Internet Zone, but left it in the My Computer zone. As such, MhtRedirLaunchInetExe simply makes it one step easier to bundle HTML, Script and executable payload in the same file.

BackToFramedJpu lets you inject javascript URLs into the history and have them executed in the context of the target window object.

HijackClickV2 lets you hijack clicks and target them at some system dialogs. You will have to know the location of those.

Threadid10008 is intended to download an HTML file to the TIF and subsequently display and parse it. It could not be reproduced on all our systems, but it does help leverage entry into a local security zones on the installations it worked on.

Locking down the My Computer security zone prevents all of the 3 exploits by mitigating the effects of the remaining vulnerabilities substantially, while still allowing a usable surfing experience.

As a final comment, I do believe that vulnerability researchers should notify vendors of potential vulnerabilities and give them some time to fix these before exposing the public to the dangers of those vulnerabilities. Posting demonstratory proof-of-concept code has served to apply pressure in the past towards unresponsive vendors, but not giving the vendors any chance to respond at all in the first place is simply irresponsible and jeopardizes the security of the Internet as a whole.

References:

[0] Qwik-Fix(r)
<http://www.pivx.com/qwikfix/>

[1]
Description of Internet Explorer Security Zones Registry Entries
<http://tinyurl.com/ubfq>

[2] Post by Liu Die Yu
<http://tinyurl.com/x8qx>

Regards

RE: Comments on 5 IE vulnerabilities

SecurityFocus Microsoft: RE: Comments on 5 IE vulnerabilities

Thor Larholm
Senior Security Researcher
PivX Solutions
24 Corporate Plaza #180
Newport Beach, CA 92660
<http://www.pivx.com>
thor@pivx.com
949-231-8496

PivX defines "Proactive Threat Mitigation". Get a FREE Beta Version of
Qwik-Fix <<http://www.qwik-fix.net>>

