

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-06/0541.html>

From: sponge (yosponge_at_yahoo.com)

Date: 06/24/03

Date: 23 Jun 2003 15:33:52 -0700

On 10 Jun 2003 19:39:22 GMT, "dkg_ctc" <dontknowguilt@hotmail.com> wrote:

>yosponge@yahoo.com (sponge) wrote in
>news:8d76ec03.0306100946.4c0d86ce@posting.google.com:
>
>*snip*
>>>And what do you use to support your claim that there is "still
>>>not sufficient bounds checking on IE's handling of IFRAMES"? A
>>>couple "vulnerabilities" which make no mention of IFRAMES?
>>
>> The flaw you cited.
>
>The flaw I cited was patched years ago...using that to claim that
>they still do insufficient checking on IFRAMES today is illogical
>at best.
>
>> Also, the flaw I posted a few weeks back in which opening more
>> than such-and-such number of IFRAMES For your edification, I
>> will repost:
>*snip*
>
>Fair enough.
>
>> It's worth pointing out that, while this particular issue was
>> patched (and I think this is what you were getting at) many
>> other issues were not.
>
>And they are IFRAME issues, right?

Do you mean the first exploit cited in my OP? It would appear so, based on the story.

Look, after re-reading your posts, it's plain to see that you don't know the first thing about security. There's more to this business than playing with programs and setting up firewalls. You also need to

know about plans, fixes, manufacturer data, and — perhaps most relevant to this discussion — usable and practical implementation methods of procedures, hardware, and software. In this case, I'm talking about the need for appropriate distribution of fixes and patches that can readily usable and that won't deter potential users from implementing them. Requiring full-blown upgrades for serious security flaws, which means time and maybe money, is poor policy, and tends to discourage the adoption of needed fixes. That's how it works in the real world. An while I never discourage anybody from using needed patches, the problem with Microsoft is that their "fixes" tend to introduce more problems.

> *snip*

>>>> *Which, incidentally, are only one version old -- legacy software, perhaps, but we're not talking about ancient history here. It is well within expectations for MS to patch such a recent version of IE.*

>>>>

>>>> *And what information do you have which supports your belief that they won't? Once again, you're making claims with nothing to back them up.*

>>>>

>>>> *History. What makes you assume that they will, naivete?*

>>>>

>>>> *Ooh, name calling, how immature...in any case, I'm not making an assumption either way. I'll leave that for you.*

Yes, you should. In the real world, software vendors do not always patch their products, and some that do have terrible methods. Witness the subject of this thread.

>> *This much is known about Microsoft: 1. they do not always patch holes in IE; 2. when they do, it is often as a part of a forced "upgrade", which may introduce new issues.*

>>>>

>>>> *And which may have less issues than older versions. Once again, you haven't provided any evidence to support that newer versions aren't more secure than previous versions.*

Nor have you provided any evidence that patched, older versions are inferior. A properly patched, older version (assuming it has fewer features) has less chance of dangerous flaws. I have already provided ample evidence of the many serious flaws with IE6.

>>>>>>>> *There is no way to "lock down" the browser; the only possible way to secure yourself from this is to discontinue using Internet Explorer entirely.*

>>>>>>>>

>>>>>>>> *Or install IE6, which as reported by your own links is unaffected.*

>>>>>>>>

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>>>>> *A large percentage of people still use pre-6 versions.*
>>>>>
>>>>> *Which says nothing regarding the fact that "the only possible*
>>>>> *way to secure yourself from this is to discontinue using*
>>>>> *Internet Explorer entirely" was completely inaccurate.*
>>>>>
>>>>> *No, actually it's entirely accurate.*
>>>>>
>>>>> *No it's not. How can you say that "the only possible way to*
>>>>> *secure yourself from this is to discontinue using Internet*
>>>>> *Explorer entirely" when there are ways to secure against this,*
>>>>> *specifically by upgrading to IE6, or following the advice that*
>>>>> *others have posted here? In fact, anyone who claims that that*
>>>>> *there's no way to secure against would appear very uninformed of*
>>>>> *the issue at hand, as there have been numerous ways to secure*
>>>>> *against this listed.*
>>>>>
>>>>> *Once again, there is apparently no fix for users of existing*
>>>>> *software, specifically, version 5.*
>>>>>
>>>>> *There are numerous fixes, including upgrading to versions 5.01,*
>>>>> *5.5 or 6.0 of IE. In fact, there have even been work-arounds*
>>>>> *posted IN THIS THREAD which will make it so you ARE NOT VULNERABLE*
>>>>> *to this exploit. You claiming that there is no fix is extremely*
>>>>> *disingenuous.*

I get your point. It's also a disingenuous point from a security perspective. There is no proper patch for existing versions. For the umpteenth time, must every bug fix require an upgrade? If we are to follow your (and Microsoft's) present logic, then yes. Download and install 10-18 megs to patch a few dozen bytes of code, and introduce more potential risks at the same time. Brilliant.

>> *Forcing users to make a major upgrade in order to be safe from*
>> *design flaws is foolish, extremely dangerous,*
>>
>> *Oh yes, it's terribly more dangerous to upgrade to a browser which*
>> *doesn't have those flaws.*

And which may introduce new ones. And does. Read those links I gave you.

>> *and smacks of malice and coercion. It's the stuff good lawsuits*
>> *are made of.*
>>
>> *Didn't you forget to add "IANAL", because it's clearly obvious*
>> *that you aren't.*

Are you sure about that?

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>> *What better way to force users to abide by some new EULA or DRM
>> scheme than to build in fundamental flaws, which can only be
>> fixed by upgrading, and thus accepting an increasingly
>> questionable agreement...*
>
>*Like I said previously, I'm not a big fan of the conspiracy
>theories.*

Generally, I am not either. But it sure would be a good long-range plan, from MS' point-of-view.

>> *More importantly, as stated in my last post, there is no
>> rational reason why a significant security flaw should not have
>> been fixed in such a relatively new version of a product.*
>
>*I'm sorry, but how is IE5.0--the version explicitly mentioned in
>the articles that YOU posted--a "relatively new version" when four
>years, three minor releases, and one major release separate IE5.0
>from today?*

It was included with Win2k. That's not exactly old, especially seeing as Win2k is a major player in business environments. Didn't you know that?

Hey, also, please explain something: why is it that Microsoft is STILL releasing patches which carry over to IE5 and 5+? And why is IE 5.01 in an Extended Support phase? That's not much newer than 5.0! They just didn't release an IFRAME patch for 5. So much for your theories.

>> *To apply your line of reasoning to the real world, it would be
>> similar to requiring auto owners to buy a new car to prevent
>> accidents due to a dangerously steering system that should have
>> been recalled.*
>
>*No, to apply that line of reasoning to the real world, it would be
>similar to a car company giving cars away for free, and then
>giving the new cars which fix flaws in the old cars away for free
>as well.*

I don't know about you, but I BOUGHT most of my computers and BOUGHT my OS with it. The only systems and OSes I didn't buy were Linux and some I did myself.

Do you really think Microsoft poured tens of thousand of man-hours -- and millions of dollars in human labor -- in order to give away it's products? Please explain, then, why Bill Gates is worth \$80 billion. Please.

Bottom line is, Microsoft produced a defective product, one with serious implications. Rather than fix it properly, they chose to force users to upgrade, and introduced even more flaws at the same time.

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>And bringing it back to the computer world, it would be similar to
>Redhat putting stopping all support after only two years. You
>want to talk about "coercien" and flaws "which can only be fixed
>by upgrading", I think you're barking up the wrong tree.

Your argument makes no sense. If I am to interpret this correctly, you believe that it would be okay for Redhat to drop support for legacy products after two years? Perhaps. That would be Redhat's problem. And, some crafty lawyer certainly could try to sue them under a variety of pretexts, and has a very good chance of being successful.

>>>> *The point is that IE is too unsafe to use in any form.*
>>>
>>>"And I'll prove it by listing 'exploits' which not only require
>>>user intervention to work, but which don't effect the last two
>>>versions (IE6 and IE6SP1) of the browsers!"
>>
>> *Kinda like "drive-by" downloads, right?*
>
>*Once again, a SEPARATE, *RELEVANT* issue unrelated to either of
>the "exploits" you originally gave.*

If you like, go ahead. Let me guess -- formatting the HD? I gave you a list of almost a dozen exploits which DO affect IE6 just as severely as 5., as well as mentioning ActiveX downloads. And THOSE exploits were just a sample of recent stuff appearing on BugTraq. So, show me some bugs that require user interaction.

>>>> *Not only was that the point of the this thread, but a point
>>>> brought up in posts of mine (and others) too numerous to
>>>> mention.*
>>>
>>>*Didn't you just get through saying that "The point was to point
>>>out flaws with some commentary"? Now you're saying that's not
>>>the point, and that the point is completely different.*
>>
>> *The point was that IE is too unsafe to be reasonably used, and
>> that it's flaws can affect other applications as well. That was
>> the point.*
>
>*"The point was to point out flaws with some commentary." Back
>pedaling, back pedal, back pedal...*

Let's see. First you were bitching that I did not explain myself or provide enough support for my statements. You posted a reply, and I explained myself further -- which is what you apparently wanted in your reply to my OP. Now you are bitching because I elaborated? Can't you get your story straight?

>> *That's pretty much been the point of the upteen IE-related posts
>> I've made in the last several years.*

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>

>*Then aren't you concerned that you might start sounding like a
>broken record?*

Well, that's why I don't post a dozen links and write long, drawn out treatises in each post. There's no need. The folks here know what's going on. Perhaps you oughtta stick around here instead of hiding out in Linux and Buffy groups -- maybe you would too.

>**snip**

>>>> *The point is that IE and it's poor coding can affect other
>>>> applications. That's one of the prime reasons I recommend
>>>> against it, and also why I have recommended both in newsgroups
>>>> and on my site that IE be locked down even if users plan on
>>>> using other browsers. I HAVE pointed out that Microsoft has a
>>>> tendency to not simply patch, but add "features" (Read:
>>>> security holes, potential exploits, etc.) in patches and
>>>> upgrades. Since ungrading to IE6 is the only way of fixing
>>>> some flaws in IE, you are dealing with the introduction of a
>>>> new set of problems.*

>>>>

>>>>*And certainly you have numbers to prove this, right? You
>>>know...the number of patches for IE5 versus IE6? Things like
>>>that? Because no offense, but so far you seem to be pulling
>>>facts from your ass.*

>>>>

>>>>*I haven't counted. If you can, go right ahead -- I have a life,
>>>you know.*

>>>>

>>>>*Yeah...like repeatedly declaring to people who are already
>>>security conscious that Internet Explorer is not safe to use, and
>>>using non-issues to then back up those declarations?*

Like backing it up with numerous reports, citations, links, quotes, etc. I suppose your idea of security is to bury your head in the sand and hope it doesn't happen to you -- that's security, right? Wrong.

<http://www.securityfocus.com/bid/7706/solution/>

<http://www.securityfocus.com/bid/7502/solution/>

<http://www.securityfocus.com/bid/7806>

<http://www.securityfocus.com/bid/7826>

Read. Learn. Enjoy your crow.

>>>> *But the FACT is that MS frequently does not patch problems, and
>>> when they do, their "patch" requires an upgrade. Again, if your
>>> logic -- and Microsoft's -- were applied to other products, you
>>> can see a whole lot more death and destruction.*

>>>>

>>>>*No, because the flaw in YOUR logic is that Internet Explorer is a
>>>FREE product, with FREE upgrades...your situation is using PAID
>>>FOR products and PAID FOR upgrades.*

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

Internet Explorer is a PAID product as one PAYS for the OS in which it is packaged and so thoroughly intertwined. One can reasonably expect support and the fixing of dangerous defects, never minding the ethical and product–liability problems.

Again, Microsoft does not produce "free" products — it takes money to produce product, and the cost is borne by purchasers of their products, like me. Perhaps you have a pirated version of Windows; I do not.

>>>> *That's not "patching".*

>>>

>>>*Not in your book, anyways.*

>>

>> *Not in most people's.*

>

>*Maybe you should stick to what you believe, and let other people
> speak for themselves, hmm? Because no offense, but if some of the
> reactions to your Kerio rules over in comp.security.firewalls are
> any indication, you really have no room to be speaking for "most
> people".*

Oh, wow! I don't know where to start picking apart this one, but thank you for presenting such target–rich foolishness.

Before I begin, for the interest of others who may be reading this, the full thread to which dkg is referring to is here (note, however, that the message from the original poster, Mike Liu, was apparently not picked up by Google, but is included in one of YK's replies.)

<http://www.google.com/groups?hl=en&lr=&ie=UTF-8&threadm=8d76ec03.0305310048.14217fc1%40posting.google>

Anyway, let me start picking apart your argument. First, you clearly have no basis to support your contention, so you resort to an ad hominem attack. What's worse than a plain old ad hominem attack is this is a complete non sequitur and is completely irrelevant to the issue at hand. And you talk about pulling things out of one's a\$\$?

But, I'll take your bait laughing my a\$\$ off. And this proves, beyond any shadow of a doubt, that you know absolutely nothing about security, because, by publishing the decrypted Kerio rulesets, I was publishing my source code!!!!

Okay, so two people don't trust my Kerio lists because, as one poster (speaking like Tracker) put it, "It's possible they [I'm a 'they?'] could be installing backdoors into kerio.?" The poster(s) Mike Liu and Dreamweaver clearly had no idea what the purpose of MD5 is — they thought it was some kind of code, and other posters as well as I tried to explain what MD5 is and the fact that my Kerio files contains them presents no security risk — indeed, they increase it. All I did was set the record straight and explain how MD5s work and basically how Kerio works, and the fact that my MD5s are in there make no

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

difference, because if your MD5 doesn't match mine, or it doesn't match null, you'd get an alert. There wasn't exactly a firestorm following my comments -- in fact, after my posting which was (incorrectly) shown as posted at 3:24 a.m., the entire subject of MD5s dropped. Oooh, what a (non) reaction!

So, since were on this subject, what have you contributed to the world of security? It would seem nothing. If anything, perhaps you're even contributing to the impairment of it by arguing that a still-fatally-flawed version of IE (6) is safer than the dubiously-less-safe IE5. (Which, if we are to follow that logic, means that it's somehow "safer" to get hacked via the ShowHelp exploit than via Exploit.SelfExec exploit -- in other words, is it better to have malicious code delivered by the former or that latter -- I got news for ya, and any security guru will tell you this, you're gonna get just as hacked either way.) Moreover, you're detracting from the overall advancement of security by advocating an arcane and ethically-questionable practice of not releasing patches for relatively current and widely-used products.

One last thing to mention: I don't care for ad hominem attacks, so I won't rake you over the coals for trolling and arguing in groups like this or comp.os.linux.advocacy in defense of MS. And, FWIW, I could make your current argument going on over there more relevant to this particular discussion than your completely irrelevant citation of a short "debate" from comp.security.firewalls, which came from completely out of the blue. However, I won't do that. But I will say this: you're not doing yourself or security in general any favors by a blind allegiance to Microsoft. Their products have their merits and their drawbacks, as does Linux, as does Opera's, as does Eudora's, and so on. But don't flip out because somebody criticizes them, because the criticism can often be constructive, and just as importantly is usually deserved. People are bitching for a reason. And, the whole reason why this debate (and, I suspect, your other debate in the Linux group) is happening at all is because -- and, again, don't take offense, as this is not meant to be insulting or derogatory, but rather constructive criticism) -- your mentality seems to be virtually identical to that of Microsoft: rather than fix a problem, foist an entirely new product on the public, be it IE6, Longhorn, TCPA, whatever. Rather than take constructive criticism and use it to better itself and its products, Microsoft would rather deny problems exist, do a rather half-assed job of fixing some of those they do acknowledge, or simply blame users, hardware, other software, and everyone else but themselves. And the previous two sentences largely explains a lot of the loathing people feel towards Microsoft and its products. And you obviously realize that there is a lot of truth in this, even though you won't come right out and admit it, because you even acknowledged that Microsoft's browser is too flawed and insecure when all is said and done. This not meant to be vituperative, only constructive.

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>> *Using a definition of "patch" that dates back at least as far as
>> Apple days (when I first saw one), a patch is a small piece of
>> code designed to fix a specific problem or set of them, not a
>> major freakin' 18 megabyte monstrosity.*
>
>*But if that "18 megabyte monstrosity" increases security by
>patching potential security vulnerabilities which may be found,
>then I would consider it a patch.*

Sure, but it makes more sense to patch an existing version with a little, itty, bitty patch than require an 18 megabyte monstrosity. Especially when that 18 megabyte monstrosity introduces brand-new flaws — putting users back at about the same level of risk.

> **snip**
>> *Try and imagine if MS required a full upgrade each time ANY flaw
>> came out! Then you'll see the total lack of logic in your
>> reasoning.*
>
>*No, I think you'll see the total lack of logic in YOUR reasoning,
>because MS doesn't do it with ANY flaw, and MS doesn't even force
>you to upgrade your browser for every flaw. Hell, the IFRAME
>vulnerability you listed above includes patches for versions of IE
>going back to 5.01.*

Wait, I'm gonna start laughing my a\$\$ off again at YET ANOTHER contradiction you made — you're whole argument has been that, if you use IE5, you should just upgrade and fix that problem, and now you're claiming just the opposite...that Microsoft doesn't require you to upgrade. Well, they do if you want to be protected from their bug! Oh, I love it. I'm glad Google is archiving this.

By the way, your statement there also reveals how wrong you are. "...MS doesn't even force you to upgrade your browser for every flaw," you said. But some. And it only takes one serious flaw to do an incredible amount of damage. Remember Sapphire?

>> *The point is that upgrading an entire browser type to fix a few
>> bytes of misbehaving code is completely without logic.*
>
>*You act as if this behavior by browser makers is limited to
>Internet Explorer, but Mozilla and Opera both do the same thing.
>But hey...might as well make this post into "Big bad Microsoft",
>right?*

Mozilla and Opera do not require payment for their products, and they are not a part of the OS. Microsoft does, and it is a part of an OS. Nor does Moz or Opera have thousands of professional programmers and billions of dollars in resources. Moz and Opera are fundamentally intertwined with the OS as is Internet Explorer.

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>>>> *In fact, one could credibly argue that Microsoft deliberately
>>>> did not patch prior versions of IE in order to force users to
>>>> upgrade to the most current version.*

>>>

>>>*By all means, feel free to argue that. I'm not a big fan of the
>>>conspiracy theories, though, nor do I think that Microsoft has
>>>any obligation to release patches for IE5, considering there has
>>>been IE5.01, 5.5 and 6.0 (and numerous service packs in
>>>between).*

>>

>> *If software products were treated by the same liability
>> standards as conventional, physical products, you bet they would
>> be obligated! Software liability law, however, is just in its
>> infancy...it should be interesting to see what happens in the
>> next few years.*

>

>*Yes, it will be interesting. However, as far as I'm concerned, if
>the software makers--ANY software makers--provide their software
>with no claim that it will or won't work securely, then that
>should be the end of it. If, as a user, you're unhappy about
>that, then take it up with the software companies by not using
>their software.*

Perhaps. I'm a little split on this issue myself. However, you ARE aware that in the real world of product liability, simply offering a disclaimer is not a significant defense against product defects. If a disclaimer was all it took for immunity, Ford would never get sued, McDonalds would never get sued, doctors would never get sued...well, we'll see.

>> *Microsot, however, can fairly be held to a higher standard that
>> Joe Smith's Software.*

>

>*Here comes the, "Oh, well, it's Microsoft, so we should treat them
>differently" argument. Thanks, but no thanks.*

Well, you're entitled to your opinion, and a judge and/or jury will be entitled to theirs.

>> *Even if we were to put the issue of the potential introduction
>> of new problems -- which you still haven't addressed -- we can
>> see that it's an unreasonable tack for Microsoft to take.*

>

>*You haven't addressed the fact that newer versions have actually
>become LESS prone to security vulnerabilities, nor do I expect you
>to.*

Less prone to EXISTING vulnerabilities. I have seen no evidence that they are significantly less vulnerable overall. In fact, let's look at your argument logically:

Given – new features are added with newer browsers, and that both are

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

patched adequately for known defects.

Old Browser –can only do HTML, JavaScript, Java

New Browser 2–can do HTML, JavaScript, Java, ActiveX scripting, ActiveX controls, VBScripting, CSS

Based on this — and assuming that the underlying code is the same, which is more likely to have known serious flaws? Give you a hint — it ain't Browser 1, because there's less there TO exploit, and because browser one was given the appropriate PATCHES (something which you are apparently against) to address it's specific flaws.

This, incidentally, is part of the reason why Opera and Mozilla don't get victimized by Drive-By Downloads, while IE does — they don't have the capability to be victimized, or at least as severely and easily. Yet Opera and Mozilla allow the download and scripting of applications if it's needed.

And there's proof in the pudding: ShowHelp exploit, which affects IE 5.01 through 6SP1, but NOT 5.0!, and the aforementioned DoS, which ONLY affects 6! As well as a number of others...

>> *Patching by upgrading may be acceptable for relatively small applications;*
>
>*Or browser-makers like Mozilla and Opera, or OS vendors like Redhat and Mandrake and Suse, or...*

Please give a citation of a Redhat bug that was cured by a full installation with no patch offered. I did not have to d/l 1.6 GB of OS last time I had to fix a bug, although I've d/led some sizeable "fixes" and minor-version upgrades.

>> *Microsoft has the resources to do things the right way.*
>
>*And so what? They have the resources, big deal. That doesn't make them any more obligated to it.*

Sure, it does. For one thing, Windows is a pricey product, so it's not unreasonable to expect better support.

> **snip**
>>>>> *Seems to me that your point was, "You can't use IE safely", and I think that's probably what any sane reader would have seen as the point, considering you actually went so far as to repeat that point. You referred to an "exploit" which requires you to download a ZIP file, open the ZIP file, and run an HTML file in the context of the local zone, and a patch which fixes security holes, as evidence that Internet Explorer can't be used safely.*
>>>>>
>>>> *The point WAS that you can't use IE safely, and I referred to two exploits: one was patched, one was not after how long.*
>>>>

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>>> *You tell me. How long? When was it first reported to
>>> Microsoft? When was it first publicly reported? It's kind of
>>> hard to claim that something is insecure when you don't even
>>> know if the vulnerability has been reported to Microsoft, isn't
>>> it?*
>>
>> *Let's see. The second item in my post was reported about mid-May
>> (still a long time!).*
>
> *A) Mid-May isn't a long time, and B) how do you know that?
> Certainly neither of the links you gave support that claim. And
> given your aversion for making claims that don't have much
> backing, you'll have to forgive me if I want actual references to
> when these vulnerabilities were reported to MS.*

For (B) I got from the article that it was two years. Kind of a long time.

>> *The first trojan was reported around the same time.*
>
> *See above.*
>
>> *IFRAME exploits go back as far as 1999.*
>
> *Yep.*

>> *BTW, upon further review, I found more info to prove you are
>> wrong in your "IE6 is immune" logic:
>> <http://www.securityfocus.com/archive/82/244242>
>>
>> "...and as stated earlier, this is a minor issue."
>>
>> *snip**
>>>> *I actually had a better link to browser-specific flaws
>>>> (including some in Opera), although I cannot find it.
>>>>
>>>> <http://www.pivx.com/larholm/unpatched/> ?
>>>>
>>>> *Nope, much better, with some good POC. I'll find it eventually
>>>> -- somewhere in 3 megs of bookmarks.
>>>>
>>>> I'll be interested in seeing it when you find it. Unfortunately,
>>>> Pivx is the only clearing house for unpatched IE vulnerabilities
>>>> that I've come across.**

Here's one you might appreciate in the interim:
<http://www.guninski.com/browsers.html>

>>>> *Nonetheless, I cited two recent and highly valid flaws.
>>>>
>>>> Highly valid to you...to me, they are non-issues which may--or*

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>>>may not--have been reported to Microsoft, and which require
>>>either out-of-date browsers (sorry, but you aren't going to
>>>convince me that Microsoft should still be releasing patches for
>>>a browser which has been out since 1999 when they've released IE
>>>5.01, 5.01SP1, 5.01SP2, 5.01SP3, 5.5, 5.5 SP1, 5.5SP2, 6.0, and
>>>6.0SP1 since that time) or user intervention. "Yeah, just
>>>download this zip and view the HTML document!! No, really, it's
>>>safe!!" Sorry, but that's not a security vulnerability.

>>

>> It it is easy enough to convince a user to download a ZIP --
>> people do every day, and unzip it via WinZIP or WINRAR using
>> browser's built-in open feature, which may not even require user
>> intervention.

>

>As far as I know, neither WinRAR or Winzip (not sure on Winzip, as
>I haven't used it in ages) open ZIPs automatically. And then,
>with at least WinRAR, the files aren't extracted until AFTER the
>one of the files is opened, at which point you don't need Internet
>Explorer anyways.

I'm think WinZIP is largely automatic. I have it installed (though I use WINRAR mostly, and have my associations set to that application). IIRC, WinZIP launched from Mozilla's download menu will only produce a dialogue box asking if you want ot run WinZIP or close, or choose a pathname.

Bear in mind that, even if WinZIP did require user intervention, it's quite easy to trick a user into believing he downloaded a "legitimate" ZIP file, and, by unZIPping it via the convenient download menu, can result in the aforementioned exploit being launched. Come to thing of it, unZIPping it into any known path should even do the trick. I've downloaded too many ZIPs to count, and unZIPped many using the download menu. So, even under the most forgiving circumstances, this is anything but an unlikely scenario.

>> Moreover, it *seems* easy enough for a redirect to take care of
>> viewing the document.

>

>Once again, I know WinRAR doesn't extract--or even open--archive
>files from a website.

No, but it does extract local ZIP archives, which, as the press release (and you) described the exploit, as doing. Therefore, any way you look at it, it's a problem. Less of a potential problem if user interaction is required, perhaps, but still a problem because it's commonplace for people to download and run an unZIPper.

>> That's hardly a process that needs lots of user intervention.

>

>If what you said was accurate, then you'd be correct. However,
>I'm not convinced that what you describe is accurate--at least,
>not for WinRAR.

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>
>>>> *And I followed up with recent BugTraq—documented flaws. Sounds
>>>> like you're sore that I'm not representing Pivx,
>>>
>>>That's not it at all. What I'm "sore" at is that people like
>>>you would rather use non—issues and vulnerabilities in defunct
>>>software to make a point, when there are plenty of VALID
>>>unpatched security holes out there. Hell, you don't even have
>>>to link to Pivx...in fact, the majority of the time, they don't
>>>even discover the vulnerabilities, they just have an archive of
>>>the ones which are unpatched.
>>
>> *Hardly defunct. Here's a little news for ya -- in RealLife land,
>> not everybody jumps on the newest Microsoft product the day it
>> comes out.
>
>Yeah, and everyone knows that IE 5.01, 5.5 and 6.0 just came out
>yesterday...**

Hmm, I still see a lot of businesses using 5.0 and the others. You see, in the real world, it's not so easy upgrading an entire company. Add to that fact the IE bugs come out on a weekly, sometimes daily, basis. For example *FOUR* were reported on SecurityFocus in the last week, and three since this thread began!! One old, the others new. And all apply only to 5.01 through 6!

>> *Not everybody jumps when Microsoft says so. Not everybody even
>> knows to.
>
>Well, seeing as how Internet Explorer is being listed in the
>Recommended Updates, I don't see how ignorance is an excuse in
>this example.*

Well, not everybody has the knowledge that we do. Unfortunately, the average Joe does not even know the threats that exist let alone can afford the services of a security professional. Again, a dose of real—life here.

>> *A browser version one—off is hardly old -- especially since MS
>> is still supporting legacy OS' like 98 (well, somewhat).
>
>Last I checked, 98SE stopped being supported last summer. That's
>not to say that you can't call up MS and maybe get pay per issue,
>but patches for 98 are no longer. Oh, and seeing as 98SE was
>released in 99 (the same time as IE 5.0), I think it's fair that
>support for IE5.0 be dead and gone.*

I had 4.0 packaged with what apparently is a fairly late edition of 98SE which is on my system. I seem to remember 5.0 being out about Me/2k time -- that's usually where I see it. At any rate, there are still a few recent patches applicable to Win98, if not designed

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

expressly for it. So, I apparently it is true that 98 is finally done.

:-)

>> *And, responsible manufacturers likewise support legacy products.*

>

>...and?

>

>> *Just because you don't like the version makes it less true.*

>

>*Like or dislike is irrelevant (although the fact that you're trying to make it look like I have a personal issue with IE5.0 in this debate is...well...pathetic). What IS relevant is that IE5.0 is four years old. It was released in 1999. Since then, there have been two minor releases (5.01 and 5.5), one major version, and numerous SPs.*

It was being sold in 2000 and, I think, even in 2001 as a part of software lying around on shelves. In any case, Microsoft should still offer patches for it -- it's not as old as you claim it to be, and IE 5 is still reasonably within the expected viable life cycle of an application. I think "life cycle" might be better way to explain the issue, and seems to be the point you're missing.

>> *There are still older versions of IE 5 out. Yes, it's true!*

>

>*And there are still old versions of Windows 95 out there too.*

>*Should Microsoft be expected to support those as well? What about old versions of Linux distros where support has ended?*

>

>> *And, thanks to this "Microsoft Mentality", they -- and, potentially, businesses and other innocent users -- because they chose not to address the issue by a proper patch, but by forcing people to upgrade.*

>

>*Yep... "forcing" people to upgrade from a four-year-old browser instead of providing patches for it. Bad Microsoft! Bad!!*

For a browser still (at least marginally) within a reasonable life cycle, yes, that's BAD!

>> *And, once again, also risking the introduction of a new set of problems.*

>

>*And, once again, you're making claims without backing them up...*

I did so profusely in past posts, in this one, and will again. Are you going to complain about my responding to your challenges again? Read up on the HtmlHelp vulnerability and others I've posted here and in the past.

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

15

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>> *Incidentally, in RealWorld-land, most people upgrade only when
>> forced to, either by a system crash which requires the
>> installation of a fresh OS, or when buying a new computer. So,
>> in practical terms, your "solution" to fixing problems is to
>> force people to lay down anywhere from \$150 for XP to \$2000 for
>> a new computer. Yes, I'm well aware that IE 6 can be downloaded
>> for free. But*
>
>*No, there is no "but" about it. IE6 can be downloaded for free.
>Period. End of discussion.*

Well, here we go again. In the real world, not everything is as cut-and-dried as you seem to think it is. Security professionals exist to address security issues to others can live their lives and not have to worry (excessively) about that crap. The average Joe does not. Nor can the average Joe afford the services of a professional. Not everybody can be a Jack-of-All-Trades, either. And, while I deeply wish more people would take online security seriously, the cold, hard reality of the matter is that the average Joe is too busy with his own life, job, and problems than to become an security whiz on the side. And I wish that people would at least take the time to educate themselves and secure themselves somewhat; I created my website for precisely these reasons. But not everybody will.

Let me explain it another way:

I also wish that everybody would take an active interest in politics, because the workings of the political world affect everybody. I wish everybody would learn to swim and possibly save their own life someday. I wish people would learn how to do basic preventative maintenance on their car to spare themselves the headache of costly repairs. But I can't -- nor have any right outside certain specific environments -- to force them to do any of the above.

The point of this little missive is that those of us in the real world recognize that, at least to some extent, these things 'just ain't gonna happen.' Not on a large scale. People have their own lives and, although you can try to educate them, there is only so much you can do. And, while I certainly feel that more CAN always be done with respect to educating people about online security -- "never give up", I say -- I'm also a pragmatist. I recognize the fact that, outside an environment I control, I can't force people to exercise good judgment, be aware of risks, and be secure.

Therefore, it entirely unrealistic to fall back on 'it's the user's fault', and expect that people will always play by the book. So-called "social engineering" attacks are all too common.

Not to mention many attacks can lure even those who do 'go by the book' to breach security, let alone attacks that don't require human intervention. People download zipfiles and executables off the net all the time -- if they didn't, we'd defeat part of the purpose of the Internet. So, it's unreasonable to say that a bug that Microsoft should have addressed in the first place is at fault here, not the behavior of hundreds of millions of people who are using the Internet for exactly the kind of purpose ifor which it is intended.

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

In the end, we've got to play the hand we're dealt, and try to strategize a little to improve our odds. Unfortunately, Microsoft is of little help -- and sometimes counterproductive -- in achieving that.

>> *out there, in the real world, most people don't voluntarily*

>> *upgrade.*

>

>*THAT'S NOT MICROSOFT'S FAULT!!*

Yes and no. Microsoft could (and does) offer a built-in feature called Windows Update and Install-on-Demand. (Which, incidentally, I'm skeptical of from an operational point-of-view, and generally recommend disabling under normal circumstances. However, they do serve a legitimate purpose and are not completely without merit -- but knowing when to enable them and when to disable them, again, is not for the faint-of-heart.) But, AFAIK, IoD doesn't work for patches and Windows Update requires manual intervention i.e. you have to recognize that occasional patching is necessary and then go do them. Don't get the idea that I necessarily favor automatic upgrades and patching. I don't, necessarily. Many software vendors and Internet-related services, and one of the most egregious of all being Microsoft, have an atrocious record privacy-wise. In fact, personally, I'd rather dispense with automatic phoning-home-for-whatever even if it serves a legitimate purpose such as patching, because the privacy implications are too severe. And, I freely admit, I don't trust Microsoft, nor most product and advertising vendors worth squat. So, at the end of the day, when all is said and done, I'd prefer to keep my privacy and endure doing updates manually, as people can be informed of the need to update via email or snail mail.

But it IS Microsoft's fault for (1) creating code that is wildly insecure (IE), (2) enabling (by default) wildly insecure features (remember File & Print Sharing? uPNP?), and (3) not offering a reasonable upgrade/patching solution (and, particularly from my point-of-view, one which respects the consumer's privacy while offering a useful service -- Microsoft does neither.)

>> *Even if they knew that they should, most don't know HOW to go*

>> *about doing it. Most don't know WHY they should.*

>

>*Yep...that big "Windows Update" is really buried in the start >menu.*

>

>> *And most are scared that an upgrade will screw up their system.*

>

>*There you go talking about what most people think/feel again.*

Comes from experience, which you clearly don't have. It's a major consideration. Heck, even I worry about the seamlessness of upgrades. I even worried about that when I "upgraded" to IE6, even though I rarely use the thing and have no important favorites or other data

Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

stored in it.

> **broken record snipped**

>> *You see, the problem here -- and the core point of what you seem
>> to be arguing in all these posts--- is that upgrading a whole 18
>> MEGABYTE BROWSER is a better solution than simply providing a
>> dinky little 500k patch.*

>

> *When it comes down to a choice between continuing patching for a
> four-year-old browser which doesn't even run on OS'es supported by
> Microsoft, and providing users an upgrade to a newer version, yes,
> I believe that providing users with an upgrade is the better
> option.*

Well, then that's an extremely dangerous mentality, especially in light of that fact that, contrary to your assertion, some OS' are reasonably current.

Incidentally, you are implying in your argument here that OS's like 98, ME, and possibly, even Win2k are "not even OS'es supported by Microsoft". Then that only proves the case I made earlier about how Microsoft is effectively forcing users to shell out \$150-\$2000 to comply with their "upgrades". And that only lends credence to the contention that Microsoft is using security flaws to gouge consumers.

>> *So, what if that logic were applied to all security fixes in IE:
>> use 36 times the bandwidth and 36 times the amount of time to
>> fix every bug in IE.*

>

> *But it's not, and you know it's not. Don't try the straw man with
> me...it won't work.*

It is in the case of the Exploit.SelfExec flaw, which you so richly pointed out. And your statements regarding Redhat, Mandrake, and SuSE, in arguing a similar point, imply the even more ludicrous acceptability of using this methodology to upgrade (in the case of Redhat) a 1.6 GB OS.

More to your point, sure, not all flaws are addressed with such massive downloads. If they were, we'd have a much worse situation on our hands. But, you have never addressed how it would have so badly hurt Microsoft to cobble together a dinky 500k patch for SelfExec exploit.

>> *And, on top of everything else, you still haven't addressed
>> another major flaw in your reasoning that I have brought up of
>> the course of several posts: an entire "upgrade" brings a new
>> set of potential problems due to the introduction or expansion
>> of features.*

>

> *Or an entire upgrade brings a new set of potential security tools
> which prevents exploitation. But you'll ignore this, point and*

alt.computer.security: Re: To Anyone who has Internet Explorer Installed or any other browser (Everybody)

>continue making the claim that newer versions are less secure.

Security tools that could have accomplished the same thing, and you'll conveniently ignore THAT point. Moreover, you'll also ignore the fact that a number of exploits DO exist that affect IE6, but not IE5. How 'bout the ClassID DoS, that ONLY affects IE6? Please explain how much better that is. Or the Fake URL vulnerability, that only affects 5.5 and 6? Or any of the others I've pointed out.

*>>>> But BugTraq is considered one of the preeminent tracking
>>>> houses in the security industry, and lists a litany of IE
>>>> flaws as well as other most other known security risks and
>>>> flaws in every kind of software.*

>>>

*>>>You're absolutely right, they are. But you didn't throw out the
>>>Security Focus links at first; you waited until someone
>>>challenged you on the issues (or lack thereof) that you
>>>originally brought up. If you'd simply used ACTUAL issues, like
>>>those listed at Security Focuse, from the get-go, then I
>>>wouldn't have thought twice. As it is, I saw you using flawed
>>>information to come to a correct conclusion; whether it'*