

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

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2003-06/0152.html>

From: dkg_ctc (dontknowguilt_at_hotmail.com)

Date: 06/10/03

Date: 10 Jun 2003 19:39:22 GMT

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?

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.*

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

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

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

> *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.

>>>>>> *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.*

>>>>>>
>>>>>> *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.

> *Forcing users to make a major upgrade in order to be safe from
> design flaws is foolish, extremely dangerous,*

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)

Oh yes, it's terribly more dangerous to upgrade to a browser which doesn't have those flaws.

> *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.

> *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.

> *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?

> *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.

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.

>>> *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.

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)

>>> *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...

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

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

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?

> *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.*

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)

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.

>>> *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".

> *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.

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.

But that doesn't really fit nicely in your view of things, so you'll undoubtedly ignore it.

> *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?

>>> *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.*
>>

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)

>>>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.

> *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.

> *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.

> *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...

> *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.

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

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)

>>>> *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.*
>>
>> *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.

> *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.

>>> *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 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.

> *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.

> *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.

>>> *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...

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

> *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.

> *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.

> *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.

> *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!!

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

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

> *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,*

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 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.

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

THAT'S NOT MICROSOFT'S FAULT!!

- > *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.

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.

- > *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.

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

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)

>>> *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 Focus, 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's a
>>correct conclusion or not, it's still flawed information that
>>brought you there, and THAT'S why I commented.*
>
> *Must I post a dozen links with each post?*

No...but it'd be helpful if you listed actual, relevant security
which don't require user intervention or browsers which are four-
years old.

*rest of the nonsense defending the choice to post two non-issues
snipped*