

Re: lets vote for better security

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security/2005-04/0434.html>

From: Roland Hall (*nobody_at_nowhere*)

Date: 04/11/05

Date: Mon, 11 Apr 2005 06:28:56 -0500

"Karl Levinson, mvp" wrote in message
news:eUiurZZPFHA.204@TK2MSFTNGP15.phx.gbl...

:

: <Vanguard> wrote in message news:YsSdnextdKaNHMMXfRVn-ow@comcast.com...

: As you know, what I and the OP wanted to be able to do is eliminate IE and

: OE-related security vulnerabilities.

That'll never happen. They're written in C++. It's an endless list.

Steve Balmer already said, in a keynote, "Well, you'd think we'd know how

to write software without buffer overflows..." (parallel) – Why isn't

everyone getting upset with AT&T for developing C and the buffer overflow to

begin with?

: It seems obvious to me that something

: is very wrong with all MS customers worldwide being required to install,

and

: thoroughly test, IE and OE patches onto production servers every 30 to 60

: days, when IE shouldn't be there in the first place.

But there is no requirement to install and update every 30 to 60 days on any
MSFT OS.

: > There are a hell of a lot of programs that rely on the HTML rendering

: > assumed available in Windows. Removing the HTML rendering engine (along

: > with the front-end UI application; i.e., the IE browser) would hurt a

: > lot more software vendors than there are 3rd party browsers claiming

: > superiority over IE.

:

: I know, but that doesn't sway me. Since most people don't use most of
those

: vendors, why should there be no possible way for such users to disable

: MSHTML?

Most people? You know what most people use and don't use? You must be very
popular. I guess that means most on NNTP are full of it most of the time.

: Giving users a way to disable IE, and/or making IE disabled by default,

: doesn't hurt those vendors at all really.

IE is part of the OS. Perhaps you'd just like a big list of enable/disable everything in an OS available to everyone. Would that make it easy? Fine. Run this app: regedit.exe.

: They would simply need to make a
: minor change to their install programs to enable MSHTML during the
: installation.

And how many more minor changes to everything affected?

: Surely you are aware that there are plenty of applications
: out there that need to enable or install other MS components in order to
: work. By extension, your argument would require every Windows computer to
: be running MSDE, etc. by default with no way to disable it, just because
: there are a lot of software vendors that use it. That would be a security
: disaster.

That's quite an extension. You must be proud. (O:=

MSDE is a security risk? Since when is an app responsible for the primary security of a system? What security model are you using?

: > I'm not saying that the IE browser is wonderful or that the HTML
: > rendering engine couldn't use some work. But, at least, it is a
: > non-proprietary document format and really shouldn't require a specific
: > front-end application to use it.

:

: I'm not saying that Mozilla is more secure than MSHTML, nor do I really
: believe that. I *am* saying that Windows is less secure because you can't
: disable powerful and risky components you aren't using, like MSHTML.

Security shouldn't begin and end with your app.

: You can't very easily argue against that,

I just did. Security is a philosophy. It's ongoing. It requires many layers.

: or if you try, you're trying to
: contradict a whole lot of security professionals.

I am a security professional and if this is their argument, I will contradict every one of them, starting with you!

: I also think it is
: entirely technically possible for MS to un-bundle MSHTML from Windows.
: Linux, Windows 3.x, etc. work just fine without MSHTML bundled in.

When did Windows 3 really work? Do you even realize what year it was when Windows 3.x came out or how many years later it took for the web to be born? (Please don't confuse web with net)

: > WSH that made the iloveyou virus and others possible gets
: > > reinstalled by a variety of install programs.
: >
: > Which is alleviated when using anti-virus software with script
: > blocking/scanning.

Which was never possible if you practiced safe computing.

: You generally block known viruses with AV. What you don't block by AV alone
: is a lone attacker in, say, Pakistan who writes a brand new script and sends
: it to your government.

Pakistanis don't write malware. They outsource it to India! (O;=

: That slips past Norton with no trouble at all.

There is no antivirus on the planet that will protect you from something it doesn't know, re: worms. It may be able to prompt for parts of your system but it cannot stop unknowns because it cannot classify them as bad.

: If your AV has good heuristics, a sandbox, etc, then your chances might improve
: somewhat and your risk might go down somewhat. But there's still risk
: there. Totally unnecessary risk.

There's always risk. You're on the net.

: Because of a technology most home users
: never ever use.

Most home users? How many home users do you know?

: Totally unnecessary. This weakens Windows security.

_____ Security is an oxymoron (put any OS in the blank)

: > like iLoveYou.

like, ok d00d whatever but I'm only attracted to wimmen! But, if you're willing to throw in dinner and a movie I may be tempted. (O;=

: Anyone not using AV software should not be connected to
: > the Internet, should not be connected to their own network, and
: > shouldn't install any software unless from a major software producer.

Perhaps you're not aware commercial software is not a safety net?!

: I use AV, and yet WSH is still a threat.

How?

: > Internet Explorer 4.0 and later treat WSH objects as unsafe ActiveX
: > controls.

Really? What zone are you referring to?

: As I recall, the default settings in the Internet security
: > zone disable initialization and scripting of unsafe AX controls. Also,
: > if you are using OE and not setting it to the default of using the
: > Restricted Sites security zone (at its default High setting) then that
: > was your deliberate choice to use lax security.

:

: None of that does anything whatsoever to block VBS files that arrive via
: NetBIOS file share, P2P, from a .ZIP file, by an attacker putting it onto
: the computer, etc. etc.

P2P? Why would you allow peer-peer in a domain model? Why is the share open? How does a vbs in a zip hurt you? Why is the system that is allowed to have access to your open as a sieve system not secure and running AV that will scan the zip? Ever hear of IPSec?

Is this how it works? Just forget all security matters and discuss possibilities that have no security applied whatsoever?

: So VBS / WSH is still a risk. I don't feel the
: user is to blame here.

The attacker is ALWAYS to blame for the incident and the user is always to blame for allowing them access. A buffer overflow may be an issue but everything else is based on config, limited by budget and knowledge.

: > WSH relies on the
: > Visual Basic Script and Java Script engines provided in Internet
: > Explorer. There are plenty of perfectly legitimate applications that
: > rely on scripting. So here you have an interdependency that most users
: > won't know about. They get rid of IE, if possible, and all of a sudden
: > some non-browser specific application stops working. The
: > interdependencies can get quite complicated and convoluted. It isn't
: > DOS anymore.

:

: That doesn't sway me either. I never said WSH or IE should be disabled by
: Microsoft post-Windows install, nor will it. It should be disabled in the
: default installation and be disable-able by Group Policy.

Group policy? How many home users are familiar with Group Policy?

microsoft.public.security: Re: lets vote for better security

: > As far as WSH getting reinstalled, guess I haven't ran into an
: > application that did that (other than service packs but that won't
: > affect script blocking/scanning by registry changes made for an
: > anti-virus program).
:
: This problem of WSH getting re-installed was a lot worse with Windows
9x...
: mainly because many versions of IE 5 - 6 containing WSH were released in
: that timeframe, while IE 6 has been largely unchanged throughout Windows
: 2000 and XP SP1. I seem to recall other apps re-installing WSH as well.

And those would be...

: > However, if one application requires it and you
: > require that application to work then it is an all or nothing
: > proposition: you enable WSH or you disable it, and enabling it means any
: > application can use it.
:
: WSH safety does not need to be all or nothing.

Well just pick what you want. You want a simple fix or a complex one?

: If Microsoft would just make
: the default action on .VBS files edit instead of execute, users would be a
: lot safer from viruses, and attackers that have not yet compromised a
: computer would in most cases not be able to call cscript.exe scriptname to
: run a malicious script.

If they can call cscript.exe, they already have access!!!

: > When running the setup program for MS Office, there is the "Microsoft
: > Office -> Office Shared Features -> Visual Basic for Applications" node
: > in the hierarchical component tree. Unchecking that option eliminates
: > installing VBA (or uninstalls it if already installed). Microsoft isn't
: > responsible for non-Microsoft programmers who do not similarly note the
: > inclusion of VBA in their installs.
:
: I don't recall seeing that option. I could certainly be mistaken about
: there not being a GUI way for a user to uninstall VBA. I'm not an expert
at
: Office XP or 2003.

... or security. (O:=

: > > Nor is
: > > there a group policy button that comes with Windows.
: >
: > I wasn't quite sure where you were going with this. A button? Maybe in
: > the Start menu?
:
: I meant that while it may or may not be possible to disable some of these

Re: lets vote for better security

microsoft.public.security: Re: lets vote for better security

: via Group Policy, you either have to download and import a MS template to do

: do, or write your own template to do so. It shouldn't be this hard to do

: something that to me seems so natural... e.g. disable functionality you

: don't need or use, both on a single system and remotely across an large

: enterprise. By "button," I meant a GUI object, such as a checkbox in a GP

: MMC console.

Some things are not easily done for several reasons:

1. They're dangerous. N00bs shouldn't have easy access. Easy access + ignorance = support call

2. If you can change it easily, so can your attacker.

I would bet "most" home users don't know what GUI represents and "most" that did would not be able to describe it. Ditto for GP and MMC, nor would they know how to access them.

Please upgrade the argument where "best security practices" have been applied and then list the possibilities. It'll make the thread more than "I think this" and "I disagree."

--

Roland Hall

/* This information is distributed in the hope that it will be useful, but without any warranty; without even the implied warranty of merchantability or fitness for a particular purpose. */

Online Support for IT Professionals -

<http://support.microsoft.com/servicedesks/technet/default.asp?fr=0&sd=tech>

How-to: Windows 2000 DNS:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;308201>

FAQ W2K/2K3 DNS:

<http://support.microsoft.com/default.aspx?scid=kb;EN-US;291382>