

RE: [Full-Disclosure] Microsoft Coding / National Security Risk

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-03/1257.html>

From: Frank Knobbe (frank_at_knobbe.us)

Date: 03/24/04

To: joe <mvp@joeware.net>

Date: Wed, 24 Mar 2004 11:07:02 -0600

On Wed, 2004-03-24 at 07:06, joe wrote:

- > [...] They weren't correcting a single
- > self-contained program like W3SVC or Apache or netdom, they were correcting
- > functionality in a core component used widely across the OS.

^^^^^^^^^^^^^^^^^^^^^^^^^^

But it's just that -- A core component. Not hundreds of core components. It was ONE DLL that needed fixin', not a multitude of them.

I think the Windows source code has grown to a size that is hard even for Microsoft to manage. I'm not surprised if the very developers are starting to lose trust in their own code because it has grown to galactic proportions... hence the need to extra long test cycles.

Regards,
Frank

- >
- > *If the next slammer virus came through and started formatting hard drives, I*
- > *would say the same thing I did when the last one came through and that would*
- > *be "How come you weren't patched with a patch that had been out that long?".*
- > *It doesn't matter how fast MS produces patches if admins and users aren't*
- > *getting them applied. The issue isn't simply one of technology, it is also*
- > *one of process. A vast number of people don't want automatic updates of*
- > *their systems either because they don't trust the source or simply don't*
- > *want their machines updating automatically but DON'T go back to do it in a*
- > *controlled fashion. They wait until someone says they need to go do it. I*
- > *don't let MS update my PC automatically but I do make it a point to go back*
- > *and check every couple of days to see if something has been released and I*
- > *watch several notification streams as well. Most people will not do this so*
- > *they either need to go with some form of automatic updates or unplug.*
- >
- > *MS sent many many people through the code. People outside are going through*
- > *the code. Again this isn't one program that one person could go through and*
- > *have a strong handle of. I don't think 10 more people could add much if any*

Full-Disclosure: RE: [Full-Disclosure] Microsoft Coding / National Security Risk

> value. Not sure 100 outside people could. If this were the case we wouldn't
> be finding old holes in other open source now, we would only be finding
> stuff in the newly released code. I would however like to think that MS is
> working on better automated scans of the code to find holes, that would be
> more value than trying to find 10 excellent security programmers. I am
> someone who has access to the current source and have walked through large
> sections of it, it isn't like the holes jump out and say "HI, here I am".
> Also the code I have had a chance to walk through in the last 8 months is
> pretty decent, I definitely am not going, oh my god oh my god. It seems more
> rigorous than the code I have walked through say for Samba however that is
> an objective opinion and am not going to enumerate items I think one does
> better than the other.
>
> BTW, how many zero day exploit based worms/viruses have been beating up on
> MS in the last year or two... Not being flip here.
>
>
> joe
>
>
>
>
> -----Original Message-----
> From: full-disclosure-admin@lists.netsys.com
> [mailto:full-disclosure-admin@lists.netsys.com] On Behalf Of Richard Hatch
> Sent: Wednesday, March 24, 2004 5:10 AM
> To: full-disclosure@lists.netsys.com
> Subject: [Full-Disclosure] Microsoft Coding / National Security Risk
>
> Hi all,
>
> Microsoft have stated that to make the source code for Windows publically
> available would be a risk to National Security.
> Microsoft also took 9 months to produce a fix for the ASN.1 problem.
>
> As much as some people may regret it, Western civilisation runs on Microsoft
> software. Imagine the panic that would ensue if the next slammer worm
> infected 10 machines then formatted hard drives, or scrambled random parts
> of random files.
> This is not news, some old DOS viruses set file lengths to zero, rather than
> deleting files that could be recovered.
>
> So my idea is this:
> Take a team of really really good C/C++ coders with excellent security
> vulnerability knowledge and have them go through the source code for windows
> (starting with the core functionality and internet facing functionality
> maybe). Find these bugs (including methodical black-box testing against the
> binaries) and fix them.
>
> These people would be fully supported by Microsoft (including full access to
> all technical documentation, Microsoft technical advisors, etc), and backed

RE: [Full-Disclosure] Microsoft Coding / National Security Risk

Full-Disclosure: RE: [Full-Disclosure] Microsoft Coding / National Security Risk

- > *by the NSA or other Government agency. Microsoft could impose whatever*
- > *NDA's they want, but they should fund the bug hunt.*
- > *Not only can they afford it, they created the problem code. Fresh insight*
- > *into how Windows functions is required to identify the less obvious*
- > *vulnerabilities.*
- >
- > *Microsoft Windows is not just another piece of software, it has become a*
- > *fundamental part of businesses and governments.*
- >
- > *Oh, can anyone suggest a reason why disclosing the source to Windows would*
- > *be a National Security risk, yet Microsoft is happy to provide the same*
- > *source code to certain third-parties (I assume this means any company that*
- > *has enough cash and signs the right paperwork).*
- >
- > *Folks, simply reacting to Odays just doesn't work.*
- >
- > *R. Hatch*
- >
- >
- >
- > ---
- > *'The mirrors have grown vast and beautiful and very very *hungry*'*
- >
- > *The views and comments expressed in this email are the personal views and*
- > *opinions of the author and should in no way be considered an official*
- > *statement/release of QinetiQ.*
- >
- > *Neither the author or QinetiQ can be held liable for actions taken based on*
- > *the information contained within this email.*
- >
- >
- > _____
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*
- >
- > _____
- > *Full-Disclosure – We believe in it.*
- > *Charter: <http://lists.netsys.com/full-disclosure-charter.html>*

Full-Disclosure – We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>

- application/pgp-signature attachment: [This is a digitally signed message part](#)