

Re: A 6% fix from Microsoft Security Bulletin MS03-040 – 828750

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2003-10/1081.html>

From: cquirke (MVP Win9x) (*name.goes.here_at_nospam.iafrica.com*)

Date: 10/06/03

Date: Mon, 06 Oct 2003 14:20:59 +0200

On Sun, 5 Oct 2003 12:17:31 -0700, "Me2" <nospam@nospam.com> wrote:

About whether MS should publicize software security defects:

- when discovered
- when fix is available
- when exploited

Several aspects to this, but I'm going to zoom in on only one of them here (and one that applies to backup as well) – negative time lines.

"Backup!" is an easy blame-the-victim mantra, but in practice it's quite a challenge, given these scope and time conundrums:

- 1) Backup must be up so up to date that you lose nothing
- 2) ...but not so up to date as to include the disaster!
- 3) Backup must be up so complete that you lose nothing
- 4) ...but not complete as to include the disaster!

In practice, one accepts some data loss, i.e. that data that was done since the most recent backup that wasn't affected by the disaster.

But what happens when the disaster is present in latent form for a long time, so that it's present within all the data you want to get back? That's what I mean by a negative timeline, and you can't address this problem unless you can:

- filter off the problem (i.e. repair)
- exclude the problem on a scope basis

Both of those workarounds involve approaches that modern Windows is arguably becoming poorer on – often the advice has been "forget data recovery or troubleshooting, given that NTFS won't let you get under the skin; just restore from backup and/or just re-install", and the blurring between data and program has made it difficult to apply risk hygiene to the data set that is to be backed up.

FTR my call is for a maintenance OS that facilitates repair and

troubleshooting within two common formality requirements:

- must run independently of HD in case HD is insane (dara rec)
- must run without running any code off HD at all (malware)

Such a mOS must also enjoy untrammelled access to everything! As one person's maintenance tool is another's hacking tool, this approach would probably be limited to XP Home only.

In fact, I'd use this as a leverage to upsell business to XP Pro. Unlike artificially limiting incoming network connections, this difference adds value to both Pro and Home.

Negative timelines apply to riak patches as well – because so far, the general assumption is that things will proceed as follows:

- 1) White-hats discover sware defect with security implications
- 2) White-hats inform MS
- 3) MS develops a fix
- 4) MS makes the fix available
- 5) MS publically announces flaw, fix, motivates patching
- 6) Black-hats discover the flaw
- 7) Black-hats exploit the flaw
- 8) Unpatched PCs spread the malware
- 9) So we must concentrate on getting patches applied

On what basis does one assume the black hats will always be slow on the draw? What if (6) and (7) happen before anything else?

As it is, hats often become grey when there's a long delay between (2) and (5). There's a dangerous perception that MS won't move on a risk until a proof-of-concept exploit is at least privately demonstrated, and from there, frustrations combined with poor lab hygiene ("Who let out the rabid rats from cage 17?" ' Not me ' ' uh-huh ' ' Nope ') can lead to (8) pretty quickly – within minutes, in fact.

My approach has been to discuss as-yet-unexploited malware opportunities quite liberally within closed forums, but not in the broader public, and part of what I hope will come of my new MVP-hood is a better channel to MS for such info.

My logic is rather like a self-imposed NDA; once it's already public knowledge, my need to stay silent is gone. But for those who need the ego-boost of being recognised as "first to discover...", the temptatration will be to speak first, or even strike first.

>-- *Risk Management is the clue that asks:*

"Why do I keep open buckets of petrol next to all the ashtrays in the lounge, when I don't even have a car?"

>-----