

Re: [ok] [Full-Disclosure] RE: [Full-Disclosure]MS should re-write code with security in mind

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-08/0945.html>

From: ASB (abaker_at_gmail.com)

Date: 08/20/04

To: full-disclosure@lists.netsys.com

Date: Thu, 19 Aug 2004 22:22:42 -0400

Well said...

-ASB

On Thu, 19 Aug 2004 11:18:00 -0300, James Tucker <jftucker@gmail.com> wrote:

- > *First of all, almost all Windows users demand backward compatibility.*
- > *While MS's software is not open source, MSDN indexes a huge number of*
- > *libraries and most all of these would have to be wrapped up to work*
- > *under a newly written OS if backward compatibility is to be*
- > *maintained. Programmers of 3rd party windows software also have a long*
- > *history of not doing things the way they should (are told to) and this*
- > *will lead to further problems if the quirks of the OS are removed.*
- >
- > *This is an issue which MS will face for years to come, and they are*
- > *trying to re-write major portions of the OS in Longhorn. SP2 was a*
- > *step in the right direction protecting most of the buffers in the OS.*
- >
- > *A drastic but potentially good option they have is actually to release*
- > *their old legacy operating systems free of charge. Source release for*
- > *MS is probably not a good idea, as alot of the source does not*
- > *change, and it is likely that many new exploits would be theorised in*
- > *a very short space of time. At least if the legacy OS's were available*
- > *consumers with legacy applications would not have so much to complain*
- > *about, in terms of lack of support and patching.*
- >
- > *There are a great deal of old DOS based applications in the world*
- > *which have yet to be rebuilt on any more modern systems; and yet to*
- > *re-install these systems it is nearly impossible these days. To find a*
- > *fresh copy of DOS is very hard now. More importantly it is even more*
- > *difficult to find a boot disk formatted with the correct generation of*
- > *boot loader.*
- >
- > *Built in encryption is available in NT and this can be hardened with*
- > *security upgrades available on MS's site. There are laws which govern*
- > *MS in this regard and restrict them from exporting high encryption*

- > OS's from the US, the specifics of which I do not know, but google
- > would be able to tell you.
- >
- > NT is a multi-user OS, it has a client server hierarchy to it also.
- > The process scheduling system in NT is a "proper" process scheduler
- > and allot of work went into changing this in Windows XP. In fact
- > certain details were changed in SP1 and it is not unlikely that they
- > changed again in SP2, although I have not heard as such.
- >
- > I am sure you are probably aware of the issues of attempting to secure
- > and authenticate all mail transfer. Authentication unfortunately
- > directly conflicts with privacy, in that if a user is to prove who
- > they are, then you know who they are. Server side authentication can
- > be useful, although this still requires some kind of centralisation in
- > order to properly authenticate. Backwards compatibility issues are
- > obvious, and more importantly you will note that holes in the system
- > will appear any time traditional plain text SMTP is allowed.
- >
- > Deep packet inspection ISP side to stop SPAM and viruses is possible,
- > however as you should be aware, being a firewall consultant, this is
- > neither fast nor cheap. The best recent solution being the regexp
- > system in Checkpoint FW1 NG+AI.
- >
- > Finally, it is not impossible for you to implement what you want
- > without MS's involvement. Theoretically there is nothing to stop the
- > community from writing an application which simply redirects all IP
- > traffic through encrypted and fully authenticated channels. This kind
- > of solution could work very effectively in a LAN scenario where all
- > machines speak the same language. On the Internet the game changes,
- > but of course, it was the Internet we were worried about in the first
- > place.
- >
- > It is true to say that closing all holes in MS software would reduce
- > the volume of SPAM and viruses on the Internet. Of course this would
- > take some time however, as many places which remain infected (which
- > contribute to most of the volume) simply would not update for a long
- > time anyway (and it is this lack of updates and security which puts
- > them there in the first place).
- >
- > If administrators and users of MS software are simply made more aware
- > of the issues which face the Internet and the professionals who
- > support it, we will slowly see a big improvement. SP2, good or bad,
- > was a step in this direction, at the very least the security center
- > will encourage users to buy / upgrade their anti virus solutions, and
- > the recompilation of major portions of the OS with buffer checking
- > will reduce the number of exploits possible in the OS.
- >
- > Software is unfortunately imperfect, and will rarely be perfect. It is
- > likely that as most systems become more secure, the viewed need for
- > vigilance on security will be lost among non IT-pro's. When that time
- > comes, it will be the rare exploits which will cause major damage, not

Full-Disclosure: Re: [ok] [Full-Disclosure] RE: [Full-Disclosure]MS should re-write code with security in mind

> *the near daily patches we see now.*
>
> *"there are no problems, only income opportunities!" –Tony Lawrence.*
>
> *my 2c.*
>
>
>
>
>
> *On Wed, 18 Aug 2004 16:00:05 –0500, Curt Purdy <purdy@tecman.com> wrote:*
> > *Clairmont, Jan M wrote:*
> > > *M\$ should just bite the bullet and re-write windows with*
> > > *security in mind, give it a true process scheduler, multi-user*
> > > *with windows as a client server processes.*
> > *<snip>*
> >
> > *It ain't gonna happen. There is so much legacy code, dating all the way*
> > *back to NT 3.5 in 2K XP that no-one really knows how it works. Of course,*
> > *that is the beauty of open-source, lots of people know how Linux works.*
> >
> > *Of course you don't have to be open-source to be secure, as Netware was*
> > *always built with security in mind. Novell engineers have a saying, "We*
> > *patch Netware twice a year whether it needs it or not." I hate to see it*
> > *go. I love SuSE linux, am running the 64-bit version on AMD, but I wish*
> > *they were keeping the Netware kernal also, for my security-critical clients.*
> > *Sadly, the days of not having to run around patching servers all the time*
> > *will be gone after Netware 7.*
> >
> > *BTW, when I have to run windows (rarely), I start a VMWare session under*
> > *SuSE, do what I need, and close it out as quickly as possible, after checking*
> > *for patches of course ;)*
> >
> > *Curt Purdy CISSP, GSEC, MCSE+I, CNE, CCDA*
> > *Information Security Engineer*
> > *DP Solutions*

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>