

Re: Security and EOL issues

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-01/msg00213.html>

- *From:* Matthew Schiros <schiros@xxxxxxxxx>
 - *Date:* Mon, 16 Jan 2006 16:50:55 -0600
-

I'd like to inject, for a moment, if I may.

I know I'm speaking from my point of view here, but I believe that what I'm about to say is consistent with what Jeffrey and others who have made similar points believe as well.

A belief that a good company, if Microsoft were one, would provide either recalls (in the case of physical products) or updates (in the case of software) to any of their products that suddenly exhibits fatally flawed behavior (in this specific instance, an easily exploitable flaw/intentional backdoor) is NOT the same thing as saying that that company is somehow responsible for the damage that may result as a consequence of that flaw (when dealing with EOL'd product lines). Microsoft is clearly in no way legally, or even ethically responsible for maintaining EOL'd code, and they are CLEARLY not liable for any damages that a system or network incur when people are using a version of their software that no patch exists for.

That's not my point, and I don't believe that it's anyone else's point. What is the point is that Microsoft was confronted with a flaw in their software that spanned all versions, and it is slightly irresponsible of them not to fix it in versions of their software that they know to still be in use. Ford doesn't support the Model T because nobody drives a Model T, and because there are a myriad of regulations governing what the automobile industry must do. Thankfully, those regulations don't exist in the software market (very much, in most sectors), so instead of asking Uncle Sam to solve the problem for us, we simply register our consumer dissatisfaction.

Is it equally irresponsible for networks to run outdated software? Yes, of course, more so. However, I can think of a myriad of reasons why you'd stay on legacy software in many environments, with cost being an obvious one, but compatibility being another. Compare that with the cost that it would have taken MS to fix the problem in NT, especially since they apparently took a fairly simple approach to it. It would have been a nice bone from a company that's been fairly anti-consumer since it first flexed its muscle.

I hope this clears up some issues. If I spoke for those who disagree

Re: Security and EOL issues

with me, I apologize.

Matt Schiros

On 1/15/06, Donald N Kenepp <don@xxxxxxxxxxxxxxxxxxxx> wrote:

- > Hi Jeffrey,
- >
- > Perhaps Steve's analogy does not fit the case perfectly. Analogies
- > usually break down at some point. Your analogy of asbestos also has major
- > faults.
- >
- > Asbestos was bad for us from the beginning. The mistake was hidden for as
- > long as possible. All this legacy software was fine to use until someone
- > else looked as hard as they could to find a problem and then exploited it..
- > Without discovery of the problem, asbestos still would have killed people..
- > Without the malicious coders, older software's security would be just fine.
- >
- > By your definition, as long as someone is using the manufacturer's
- > product, the manufacturer is liable for that person's usage of their
- > product. This is not actually the case.
- >
- > In new products, we see a product recall, with free replacement or repair.
- > This is essentially one part of service packs. In legacy products, we see
- > them removed from the shelves, often replaced with a better product. You
- > cannot purchase Windows NT 3.11 from Microsoft anymore, just like you cannot
- > purchase a Model T. Ford is no longer responsible for your safety if you
- > choose to still drive a Model T. They aren't responsible for your safety if
- > you choose to drive a car without safety glass, breakaway steering wheels,
- > or seatbelts.
- >
- > At what point are you willing to say that because Microsoft has removed
- > Windows NT 4.0, Windows 98, and Windows Me from the shelves, because they
- > have declared these products EOL with an extended support grace period, and
- > because they have given warnings about their core security design being
- > outdated by widespread availability of current malicious software
- > technology, that Microsoft is no longer responsible for your insistence on
- > using that legacy product?
- >
- > Would you expect a security company to still be liable for your home after
- > they have noted their outdated model security system has a security box that
- > is no longer sufficient since a tool has been developed to break in that is
- > now readily available to neighborhood thugs? Should they still be liable
- > when their outdated security system has been removed from the shelves and
- > labeled as EOL for several years? Should they still be liable if their
- > outdated security system has been replaced on the shelf by a new security
- > system for which you can obtain a discount on installation since you are
- > being "forced" to upgrade rather than trying to patch the old system?
- >
- > Would you expect every car company to develop and offer free OEM upgrade
- > kits to electronic locks and satellite tracking systems for their outdated
- > models with locks and windows susceptible to coat hangers or else be liable
- > for the theft of your car?

Re: Security and EOL issues

Re: Security and EOL issues

>
> Should the car companies have to replace your electronic key every time
> someone builds and distributes a new scanner which breaks their encryption,
> or should they be responsible for attempting to resolve this issue on new
> cars and try to stay one step ahead of the bad guys for a little while, lest
> they lose new buyers?
>
> At what point is it the consumer's fault for insisting on using something
> outdated, no longer available from the manufacturer, and proven to be easily
> compromised by advances in the anti-security field?
>
> Stop trying to lock your door with the same old hook and loop just so you
> can complain that the people who sold you your home should ship you a
> deadbolt for free.
>
> Sincerely,
> Donald
>
>
> -----Original Message-----
> From: Jeffrey F. Bloss [<mailto:jbloss@xxxxxxxxxxxxxxxx>]
> Sent: Thursday, January 12, 2006 8:17 PM
> To: security-basics@xxxxxxxxxxxxxxxx
> Subject: Re: Security and EOL issues (was RE: WMF Exploit Patch released)
>
> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> On Tuesday 10 January 2006 02:41 pm, Steveb@xxxxxxxxxxx wrote:
>> Hi all,
>>
>> I must weigh in on this with an analogy. Asking software companies to
>> offer free patches to software whose core technologies are considered
>> out of date by the mainstream industry is like asking Ford Motor company
>> to offer free airbag installations in all 1920 vintage automobiles.
>
> Not really, for a couple of reasons.
>
> If a flaw exists in a piece of software a "core" technology must exist too.
> 1920 era vehicles lack the modern electrical systems and physical features
> that allow air bag installation without extensive modification to the
> automobile itself. A software patch or bug fix, by definition, is something
> that only modifies an existing "part". Your analogy would be more like
> expecting Microsoft to upgrade Notepad so that it was identical to Word.
>
> Installing air bags requires that the automobile manufacturer design, test,
> and produce the upgrade. As does a software patch. But in the automobile
> scenario no typical end user is going to be able to order the parts and
> perform the work themselves. Unlike software patches. There's an entire
> "implementation" phase of fixing automobiles that simple does not exist in
> the world of software. In fact, as we just saw first hand the fix can be

Re: Security and EOL issues

> manufactured, packaged, and implemented at little or no cost at all. Even
> by third parties. :)
>
>> The rest of the capitalist world protects themselves from such
>> expectations in the form of limited time warranties. Why should the
>> software world be any different?
>
> This too is a flawed analogy. We're not talking about adding features or
> functionality, or fixing something that wears out through normal use. We're
> talking about fixing flaws and errors. The capitalist world most definitely
> does find itself liable for problem in products that are no longer
> supported.
> A glaring example would be asbestos.
>
> If a significant number of people still drove 1920's era vehicles, and a
> major
> design miscalculation like wheels falling off due to the usage of superballs
>
> instead of ballbearings were discovered, it's a pretty safe bet Ford would
> be
> "patching" a significant number of their 1920's era automobiles.
>
> Yes, it's a silly example, but the point is that product vendors are
> accountable for their mistakes long after their advertised warranties
> expire.
> If a flaw that impacts the end user's "safety" is discovered, a manufacturer
>
> is almost always held accountable and required to make things right.
>
> Why should the software world be any different? :)
>
> ---
> Hand crafted on January 12, 2006 at 19:35:31 -0500
>
> Outside of a dog, a book is a man's best friend.
> Inside of a dog, it's too dark to read.
> -Groucho Marx
> -----BEGIN PGP SIGNATURE-----
> Version: GnuPG v1.4.2 (GNU/Linux)
>
> iD8DBQFDxv90RHqalLqKnCkRAhXCAJ0SjrITxOk1F9QR6hF09EJS0lshMACeMtEP
> 15QXrab8r5FA4cw/jR9d3rk=
> =TpIK
> -----END PGP SIGNATURE-----
>

> EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE
> The Norwich University program offers unparalleled Infosec management
> education and the case study affords you unmatched consulting experience.
> Tailor your education to your own professional goals with degree
> customizations including Emergency Management, Business Continuity Planning,

Re: Security and EOL issues

- >
- > Computer Emergency Response Teams, and Digital Investigations.

- >
- > <http://www.msia.norwich.edu/secfocus>

- >
- >
- >
- >
- >

- > EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE
- > The Norwich University program offers unparalleled Infosec management
- > education and the case study affords you unmatched consulting experience.
- > Tailor your education to your own professional goals with degree
- > customizations including Emergency Management, Business Continuity Planning,
- > Computer Emergency Response Teams, and Digital Investigations.

- >
- > <http://www.msia.norwich.edu/secfocus>

- >
- >

EARN A MASTER OF SCIENCE IN INFORMATION ASSURANCE – ONLINE

The Norwich University program offers unparalleled Infosec management education and the case study affords you unmatched consulting experience.

Tailor your education to your own professional goals with degree customizations including Emergency Management, Business Continuity Planning, Computer Emergency Response Teams, and Digital Investigations.

<http://www.msia.norwich.edu/secfocus>

• *Follow-Ups:*

- ◆ **Re: Security and EOL issues**

- ◇ *From:* Robert Newton

- ◆ **RE: Security and EOL issues**

- ◇ *From:* Donald N Kenep

• *References:*

- ◆ **Re: Security and EOL issues (was RE: WMF Exploit Patch released)**

- ◇ *From:* Jeffrey F. Bloss

- ◆ **RE: Security and EOL issues**

- ◇ *From:* Donald N Kenep

- Prev by Date: **Re: User access management**
- Next by Date: **RE: Anti-Virus**
- Previous by thread: **RE: Security and EOL issues**
- Next by thread: **RE: Security and EOL issues**
- Index(es):

Re: Security and EOL issues

- ◆ Date
- ◆ Thread