

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2006-02/msg00041.html>

- *From:* Jude DaShiell <jdashiell@xxxxxxxxxxxxxxxx>
 - *Date:* Mon, 30 Jan 2006 23:32:24 -0500 (EST)
-

Why not set up paid upgrade systems using annual contracts? The commitment on the contract is to continue to support as long as contracts are paid with the restriction that the needed support must be technically feasible and as timely notification as is possible when support is not technically feasible will be provided. I remember one company that had in its contracts once it provided a system that the user's systems which included both software and hardware would be kept current for the term of the contract. Perhaps in the future if hardware costs decrease enough, you won't buy software anymore but systems that is an operating system comes with what it will run on and the vendor acquires the responsibility to keep you current for the term of your contract. For now no problem for well-funded corporates could be same would be possible for individuals in future.

On Tue, 10 Jan 2006, Steveb@xxxxxxxx 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 Asking software companies to offer free patches to software whose core technologies are considered out of date by the mainstream industry is like asking Ford Motor company to offer free airbag installations in all 1920 vintage automobiles.

While I sympathies with those that feel that Microsoft is getting richer by forcing upgrades in the name of tighter security, I really don't see that as much of an ethical issue when looked at in light of how the real world works. In what other industry do we expect unlimited free upgrades like we do from the computer software industry?

Don't get me wrong, I LOVE free upgrades and free bug fixes! I just have to balance that with the realization that if the equipment that I'd like to have a bug fixed on is out of date, I can't expect the manufacturer to fix it for free.

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?

Steve Bostedor
Boztek VNCScan Enterprise Manager

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

<http://www.vncscan.com>

-----Original Message-----

From: Donald N Kenepf [<mailto:don@xxxxxxxxxxxxxxxxxxxxxx>]

Sent: Sunday, January 08, 2006 9:33 PM

To: 'Matthew Schiros'

Cc: info@xxxxxxxxxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxxx

Subject: Security and EOL issues (was RE: WMF Exploit Patch released)

Hi Matthew,

Perhaps I was too harsh in my response. I understand your argument that since Microsoft does not give others their source code, they should be fully responsible for maintaining the code. At the same time, they have decided that rather than continuously patching the same piece of software, they are going to do a major rewrite every three to five years and sell it as a new system.

Some bugs are design flaws that simply cannot be patched. This is why no matter whether we choose closed or open-source, we always have to apply a certain amount of maintenance to our software. With open source, we are largely responsible for ourselves from day one. While we assume major flaws will be repaired, there is no guarantee that a fix will ever be released.

With closed source, we can demand someone else fix it for a reasonable in a reasonable timeframe for a reasonable amount of time. Eventually the time and effort involved in patching something rather than replacing it is simply not efficient, and in both cases, that someone else will stop doing so. The only relief with open source is that if no one but you cares, you can still try to do it yourself.

You are correct that I should not be addressing this as being directly about the age of the OS. This is not about patching vulnerabilities due to the age of the OS, but rather due to the changes since this version of the OS and other advancements in that time. Compare AIX to Windows, and AIX version X to Windows version X. I do not know the AIX system model, but it seems to have obsolete versions as well. IBM ended software support for AIX Base Operating System 4.3.3. Perhaps IBM still does release fixes for security flaws in 4.3.3 even though they have declared its EOL. Does it still release fixes for 3.2? I would not fault them for no longer supporting their older kernel versions past a reasonable transition.

Eventually it becomes too much overhead that is better spent elsewhere.

Every vendor releases new builds and patches, and inevitably there are versions that should not be used because they are known to be vulnerable and have been replaced. I believe you will find that any operating system, just like any other software program, has a point at which they are no longer supported. Should Adobe still be held responsible for fixing security issues in Acrobat 3?

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

It may be that developers or third-party vendors stop supporting the older OS version. In the case of open-source, a version is basically no longer supported when the vast majority of the open-source community simply stops trying to fix the old material and works on something new. I am sure there are kernel bugs and security flaws that will never be found, exploited, or patched for the Linux 2.0.0 kernel. Linus has passed off everything prior to 2.6.x to other maintainers, and most new software expects you to use 2.4.x or 2.6.x.

At what point should we start over rather than fixing fatal flaws? Should Microsoft be putting time and effort into fixing fatal flaws in Windows NT 3.x as well? At what point would you rather IBM focus on future development than spending time to fix a fatal flaw in AIX 4.3?

If we are still using NT 4.0 on mission critical machines, we need to ask why we are doing so. What is our obligation to our customers to use current software on mission-critical machines? How much are bandages and the time it takes to put them on costing us against the cost of a new system that doesn't need as many bandages? I push to get users and companies off of operating systems that are obsolete, whether because they have security exploits, because they are no longer cost effective to maintain, or because they are no longer supported. Sometimes I win, sometimes not, but I always try.

It doesn't matter whether we choose to move to open source or the next Microsoft product; we shouldn't be using a system at the end of its life if at all possible. While WMF may be a high priority at the moment, I would honestly say that the security design improvements and other general improvements to the NT family since NT 4.0.SP6a should have been a high priority before now.

To your question regarding the NT 4.0 seg fault, Microsoft does still have what they call "critical updates" for NT 4.0. They do not feel that the WMF flaw meets their definition of a critical flaw for NT 4.0, so they may not put the extra effort forward until such point it meets those criteria.

While it would be nice if NT 4.0 was easily fixed and happened to be patched along with everything else, it isn't worthwhile to fix NT 4.0 bugs anymore at the cost of forward progress. Microsoft threw a lot of weight at this patch. Should Microsoft have held the WMF patch release until there was a fix for NT 4.0 and Windows 98? Should they work 24/7 on a patch for them now? How much weight is reasonable to throw at those older systems?

Perhaps it would be easier to see if rather than having names like Windows 2000, XP, and 2003, we noted they are all NT version 5.x. The Microsoft product timelines might also be helpful:

<http://www.microsoft.com/windows/WinHistoryIntro.mspx>

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

Getting rid of NT 4.0 seems like something drastic because it is arguably the first widespread and long-lived corporate version of Windows to be EOLed. I really wouldn't refer to it as a huge campaign for years followed by a quick EOL, however. It's been patched for almost a decade with six major service releases and countless hotfixes. There was at least a year of warning about its EOL, followed by an extra two years of extended support due to high customer demand and agony over it being the first major EOL announced. This isn't under the blanket of ending support; it's under the blanket of long since ended support. Almost all software written for NT 4.0 still works on newer versions of the OS. The reason we don't see patches anymore is because the new OS versions are becoming so different that usually the same patch doesn't work for both, or only NT 4.0 requires the patch.

I can understand skipping Windows 2K Server if you worried about it as a beta for Active Directory. I hope you skipped Windows Me. I understand budget issues and upgrade nightmares.

I believe Windows Vista is NT 6.0, putting NT 4.0 two major kernel versions and several NT 5.x releases behind. The question becomes how long you want your vendor to support each version of the products they release, and how much effort you want them to put toward the older releases. I am glad Vista/Longhorn/Blackcomb was delayed for XPSP2 (NT 5.1's major security revision) because it marked the beginning of a huge turn-around in security efforts from Microsoft. I don't feel things should be similarly delayed for patches to NT 4.0.

Sincerely,
Donald

-----Original Message-----

From: Matthew Schiros [<mailto:schiros@xxxxxxxx>]
Sent: Saturday, January 07, 2006 11:22 PM
To: don@xxxxxxxxxxxxxxxxxxxxxx
Cc: info@xxxxxxxxxxxxxxxxxx; security-basics@xxxxxxxxxxxxxxxxxxxxxx
Subject: Re: WMF Exploit Patch Released

Donald,
Perhaps I chose my words poorly. My point was not that Microsoft was using this patch as an attempt to push users away from NT 4.0. I know that NT 4 was has been EOL'd for some time now, and I'm aware that there are many viable replacement OS's put out by Microsoft since. At the same time though, there's the issue of taking responsibility for your software when you aren't willing to reveal the source and allow others to make the fixes that you aren't willing to. This isn't a matter of a low-risk bug in a piece of legacy word processing software, it's a highly dangerous exploit in software that, if its being used today, is used on what's likely mission critical machines.

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

While I'd like to say that MS can't have its cake and eat it too, it can. It can spend years pushing a product, get everyone to use that product, and then relatively quickly EOL that product, and get you to move to something else. It's a great business model, obviously, because people keep buying, but at the same time, how many System V or AIX exploits do you think appear that go unfixed because of the age of the OS? What kind of relationship do you have with your customers if you just refuse to take responsibility for a drastic flaw under the blanket of ending support? Nobody is saying that Microsoft should be obligated, or should even consider, doing anything like doing DirectX updates or anything, just fix fatal flaws in already existing code. If it suddenly turned out that NT 4.0 seg faulted every time it recieved an incomplete TCP packet (obviously this isn't the case, but whatever), would you say that Microsoft had no obligation to fix that problem?

Matt

On 1/7/06, Donald N Kenep don@xxxxxxxxxxxxxxxxxxxx wrote:

Hi Matthew,

Sadly, it isn't so much Microsoft saying you should upgrade for this

patch, but Microsoft saying you should have upgraded from Windows NT 4.0 a long time ago. NT 4.0 has been being retracted from the market since

2001.

It was declared closed for normal support in 2003. They are now phasing

out

extended support in 2005. Windows NT 4.0 first showed up back in

1996.

We

have since had 98, Me, W2K, XP, and now Vista is coming. The server end

has

seen W2K and 2003 with a service pack. Should an OS be supported for ten years past its inception?

Will there be a WMF patch for Windows 95 as well? One way to look at things is that Microsoft is an evil empire sticking it to the man.

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

One might also say they are the average business with new products.

Regardless of motive, it honestly costs more to maintain NT 4.0 at this point than to upgrade to a newer OS. Red Hat 4.0 also came out

in 1996.

The amount of patching, manual configuration, and manual administration involved in a product that has seen its day come and go

is much more expensive than migration. There is also a fair amount of

default

security,

productivity, and usability gains in the newer versions of these

products.

You can still run programs dating back to Windows 95 and NT 4.0 and even DOS on Windows XP. That's a lot of overhead Microsoft built in to ease transitions. Skipping one OS version for cost reasons can certainly make sense, but if you are making things last and your workstations and servers have a five year lifecycle, so should their

operating systems.

Just for some perspective on 1996:

Dell opened internet sales.

Netgear was founded.

Google was first developed.

Sony entered the PC market.

Microsoft introduced Windows NT 4.0 and Windows CE 1.0.

Sun introduced the Ultra workstation family and licensed Java.

Seagate released the original 10k Cheetah drives at 6GB.

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

Intel released the 200MHZ P6. The 266MHz PII didn't come until 1997.

I do wish you the best of luck in patching NT 4.0 systems if you are

truly

stuck with them, but my recommendation to anyone still on NT is to use

this

as one more reason to present the idea of a new OS to management this

year.

Sincerely,
Donald

-----Original Message-----

From: Matthew Schiros [<mailto:schiros@xxxxxxxx>]

Sent: Friday, January 06, 2006 12:47 PM

To: info@xxxxxxxxxxxxxxxx

Cc: security-basics@xxxxxxxxxxxxxxxxxxxx

Subject: Re: WMF Exploit Patch Released

According to Microsoft, WinNT4 and Win2k SP3 users are out of luck. Their recommended "solution" is to upgrade your software to a supported version. Obviously, all this means is that they have no solution at all, but this is hardly the first time that MS has stuck it to WinNT4 users as part of an attempt to get them all moved over to

2k SP4. As for the viability of disabling the DLL's in question, while I haven't had any problems as a result of doing that on the 2k boxes in the office, I haven't had the opportunity to test its impact on NT systems. That seems to be the only way of removing the exploit from your machines though, and I'd be interested in knowing the results of your attempts.

On 1/6/06, info@xxxxxxxxxxxxxxxx <info@xxxxxxxxxxxxxxxx> wrote:

Hello Everyone,

Unfortunately there are company who are still running NT4 and I was wondering which alternative do they have

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

to face this security breach from the fact that Microsoft do not provide

any

patch for NT4 .

Do they have to disable GDI32.DLL and WGDI32.DLL as suggested previously

for

SHIMGVW.DLL?

Regards.

Ernest Matos

IT Security

-----Original Message-----

From: Matthew Schiros [<mailto:schiros@xxxxxxxxxx>]

Sent: Thursday, January 05, 2006 10:51 PM

To: security-basics@xxxxxxxxxxxxxxxxxxxxx;
bugtraq@xxxxxxxxxxxxxxxxxxxxx

Subject: WMF Exploit Patch Released

Microsoft has released a patch for the WMF exploit a couple of days

early, apparently due to a faster-than-expected testing process, and,

at least I hope, some consumer pressure. It can be downloaded via

Windows Update, or as a standalone install at:

<http://www.microsoft.com/technet/security/Bulletin/MS06-001.msp>

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

As a note, it appears that all of the attempts to circumvent the problem via disabling SHIMGVW.DLL were irrelevant, and that those who discovered that GDI32.DLL and WGDI32.DLL were the culprits were correct.

Happy crawling.

Matt Schiros

Web Developer

Academic Superstore

www.academicsuperstore.com

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

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

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

RE: Security and EOL issues (was RE: WMF Exploit Patch released)

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>

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>
