

Re: Vista's Security Rendered Completely Useless by New Exploit

Source:

<http://www.tech-archive.net/Archive/Vista/microsoft.public.windows.vista.general/2008-08/msg03872.html>

- *From:* johngalt <guest@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Tue, 12 Aug 2008 01:23:50 -0500
-

And more:

Ed Bott had already written a previous blog about this :

"<http://blogs.zdnet.com/Bott/?p=512> Wrote:

'*Windows security rendered useless? Uh, not exactly*
Ed Bott's Microsoft Report | ZDNet.com'
(<http://blogs.zdnet.com/Bott/?p=512>)

-Update 11-August, 6:00PM: Don't miss my 'exclusive follow-up
interview' (<http://blogs.zdnet.com/Bott/?p=513>) with researcher
Alexander Sotirov, who says 'The sky is not falling and the flaws
are not unfixable.'

Oh dear. The Chicken Little contingent is out in full force. Break out
your Kevlar helmets, everyone, because the sky is falling on Windows! At
last week's Black Hat conference in Las Vegas, researchers
Alexander Sotirov and Mark Dowd presented a paper that outlined some new
attack vectors they had discovered targeting some security features
introduced in different versions of Windows XP and Windows Vista.
It's a fascinating paper, rich in technical detail and hewing to
the Black Hat tradition of providing clues that others can follow to
discover, exploit, and ultimately fix vulnerabilities in widely used
computer code.

Unfortunately, most people who read about Sotirov and Dowd's
work didn't bother to read the technical paper. Instead, they
relied on quick summaries, most notably the one provided by
SearchSecurity, which was picked up by Slashdot and our own Adrian
Kingsley-Hughes. Alas, those stories are wildly inaccurate and
hopelessly sensationalized.

The 'rendered useless' quote is in the headline from
SearchSecurity's article, which 'breathlessly asserts'
(http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1324395,00.html):

Re: Vista's Security Rendered Completely Useless by New Exploit

Researchers who have read the paper that Dowd and Sotirov wrote on the techniques say their work is a major breakthrough and there is little that Microsoft can do to address the problems.

I'll skip right over the implication in that first statement, that the author of the SearchSecurity article hadn't yet read the paper and was instead relying on second- and third-hand accounts. As for the contention that there is little that Microsoft can do; maybe we should ask Sotirov and Dowd, who conclude their paper with this matter-of-fact statement:

The authors expect these problems to be addressed in future releases of Windows and browser plugins shipped by third parties.

The 'rendered useless' meme was picked up by 'Adrian, who led off his story' (<http://blogs.zdnet.com/hardware/?p=2387>) with this alarming oversimplification:

So, in a stroke, two security researchers (Mark Dowd of IBM and Alexander Sotirov of VMware) at Black Hat have set browser security back 10 years and rendered Vista's security have been rendered useless; -[sic]- I'm surprised that it took this long for the walls to come tumbling down, but I have to admit I didn't expect all of them to come down at once like that!

And then, three paragraphs later, he notes, 'The sky isn't falling in.'

OK, so which is it? One clue is that Adrian's piece doesn't include a single quote from the original paper. It has no discussion of the exploit techniques as described by the authors, nor does it include any commentary from the authors or from anyone who saw their talk in Las Vegas. Instead, it echoes the wording of the SearchSecurity article.

If you read the authors' actual words, not the sensationalist and wildly inaccurate news accounts, you get a completely different story. Here's how the 'authors describe the talk' (<http://taossa.com/index.php/2008/08/07/impressing-girls-with-vista-memory-protection-bypasses/>) they gave at Black Hat, for example:

Specifically, we will be discussing how rich browser functionality can be utilized to help lessen the impact of memory protections (and in some cases, completely negate them). Some of the techniques we will be discussing are known ones, whereas others are new approaches that we haven't seen discussed in public forums before.

Memory protection is one part of a comprehensive, multi-layered approach to security. Microsoft calls this approach 'defense in depth' and specifically makes the point that features like this will always be under attack and will eventually be

Re: Vista's Security Rendered Completely Useless by New Exploit

defeated. If you don't believe me, listen to Microsoft's Michael Howard, security expert and author of Writing Secure Code, who 'predicted this back in 2006' (http://blogs.msdn.com/michael_howard/archive/2006/06/12/628207.aspx):

There are two overarching goals at work; the first is to reduce the number of bugs in the code, and the second is to make it harder to reliably exploit any bugs that remain. [W]e can do the very best we could possibly do, but Windows Vista will be in the market place for years and in that time, I can guarantee new attack techniques will be discovered, as will new bug types, and we can't necessarily anticipate the future. Also, our tools are not perfect; we know they won't find all vulnerable code. With that in mind, we must add other defenses.

So how does defense in depth work? Well, an attack has to start with code that exploits a system vulnerability, such as buffer overrun that allows an attacker's code to execute on a target machine. The victim has to be induced to actually run that code (in this case, by visiting a booby-trapped web page). The example that Sotirov and Dowd use is the ANI cursor vulnerability, which was 'unveiled' (<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0038>) and 'patched' (<http://www.microsoft.com/TechNet/security/advisory/935423.mspx>) in early 2007. The best defense against this type of vulnerability is to fix it before it's released; the next layer of defense is to quickly patch vulnerabilities like this after they're disclosed. Well-written antivirus software can identify and block specific exploits and can also detect and stop generic attacks. What Windows Vista adds to the mix is a set of memory protection features that make it more difficult for attackers to run code remotely. Note that I said Ümore difficult,Ý not Üimpossible.Ý

The sensationalist stories about this paper start with the amateurish viewpoint that memory protection was designed to be an infallible security barrier. Security professionals inside and outside Microsoft know otherwise. One of the biggest targets of the work by Sotirov and Dowd is Address Space Layout Randomization (ASLR). When Michael Howard first wrote about ASLR back in 2006, he specifically cautioned against thinking of it as a magic bullet:

Windows Vista Beta 2 includes a new defense against buffer overrun exploits called address space layout randomization. Not only is it in Beta 2, it's on by default too. Now before I continue, I want to level set ASLR. It is not a panacea, it is not a replacement for insecure code, but when used in conjunction with other technologies, which I will explain shortly, it is a useful defense because it makes Windows systems look ÜdifferentÝ to malware, making automated attacks harder. [[#230;](#)]

ASLR is seen as just another defense, and it's on by default in

Re: Vista's Security Rendered Completely Useless by New Exploit

Windows Vista Beta 2. I think the latter point is important, we added ASLR pretty late in the game, but we decided that adding it to beta 2 and enabling it by default was important so we can understand how well it performs in the field. By this I mean what the compatibility implications are, and to give us time to fine tune ASLR before we finally release Windows Vista.

[#8230;]

Ok, let's assume that the attacker has the motivation, time, patience and expertise to bypass all these defenses. There's more! A new defense for Windows Vista is 'Service hardening' (<http://www.microsoft.com/technet/windowsvista/evaluate/feat/secfeat.mspx#EHF>). It's a broad subject, so I want to focus on just two parts of service hardening. The first is the ability to describe the privileges that a service requires, and the service control manager (SCM) will assign only those privileges to the process. #8230; The exploit code runs with the same privileges as the host process, and reducing the privileges associated with the process means the exploit code can do less damage. Of course, there may very well be privilege elevation bugs in Windows Vista that we do not know about, but in my opinion it's better to put up defenses, rather than no defenses at all.

That's the best summary I've read in a long time of the cat and mouse game that is modern computer security. Software developers do their best to design systems that have a solid baseline of security, and then they add features that make it more difficult for attackers to succeed in breaching the system. Attackers (black and white hats alike) poke and prod at those systems to find new vulnerabilities, which the software designers in turn have to deal with in current and future releases.

So, where is Windows 7 in all this? As Michael Howard noted in his ASLR announcement from early 2006, the ASLR feature was added fairly late in the development cycle to Windows Vista. Microsoft's security team has been working with and refining ASLR for more than two years. The idea that they've been completely blindsided by the revelations in a single Black Hat paper and that they'll have to scrap the entire architecture of the Windows platform is naive, to put it charitably.

-Update: Peter Bright at Ars Technica has 'an excellent post'

(<http://arstechnica.com/news.ars/post/20080811-the-sky-isnt-falling-a-look-at-a-new-vista-security-byp>) on the same subject, hitting many of the same themes-:

Sensationalism sells, and there's no news like bad news, but sometimes-; particularly when covering security issues-it would be nice to see accuracy and level-headedness instead. Alarmism helps no one. Responsible vulnerability disclosure is a big concern in the security industry; it would be good to see it coupled with responsible reporting.

The work done by Dowd and Sotirov focuses on making buffer overflows that were previously not exploitable -on Vista- exploitable. These are buffer overflows that would be exploitable on Windows XP anyway; after all, there's no need to defeat ASLR if an OS does not have ASLR at

Re: Vista's Security Rendered Completely Useless by New Exploit

all. Furthermore, these attacks are specifically on the buffer overflow protections; they do not circumvent the 'IE Protected Mode' (<http://arstechnica.com/reviews/os/vista-under-the-hood.ars/2>) sandbox, nor Vista's (in)famous 'UAC' (<http://arstechnica.com/reviews/os/vista-under-the-hood.ars/1>) restrictions. DEP, ASLR, and the other mitigation features in Vista are unlikely to ever be unbreakable, especially in an application like a web browser that can run both scripts and plugins of an attacker's choosing. Rather, their purpose is to make exploitation more difficult.
'-Go read the whole thing.-'
(<http://arstechnica.com/news.ars/post/20080811-the-sky-isnt-falling-a-look-at-a-new-vista-security-byp>)

==
johnlgalt

<----- -If you found my post meritable, show me!

- *Please do not contact me via PM or IM for help - post it in the forums so that others may benefit from

:cool:

CPU: Core 2 Quad 6600 G0 CPU @3.375 GHz

Heatsink: Tuniq Tower 120 LFB Cooler

Motherboard: eVGA 780i Motherboard

PSU: OCZ ModXStream 780W SLI Ready PSU

Graphics Card: eVGA 8800 GTS 512 KO edition GA

RAM: 2 X 2GB OCZ PC2-8000 ReaperX HPC RAM @ 500 MHz (1000 MHz Dual)

HDs: 2 X Seagate 500 GB 7200.11 RPM 32MB Cache HDs

Optical: SONY DRU-830A Dual Layer IDE DVD burner

Extra: Hauppauge WinTV 1800 HVR TV Tuner card with Remote

Case: ThermalTake Armour case

Monitors: Dual Acer X312Wbd 21.6" Widescreen Active Matrix TFT with 2500:1 DC

<http://picasaweb.google.com/johnlgalt/TheBeast>

.