New Vulnerability & Exploit Unveiled for Windows 7 & Windows 8

Once again, a Microsoft operating system has a new zero-day exploit. That should not come as any earth-shattering news, since Microsoft's Windows operating system has had numerous vulnerabilities and exploits over the years, exposing all of us that use their software.

What does make this development significant is that it comes after much effort and many reassurances from Microsoft that they've made Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012 far more secure.

Even more interesting is that Microsoft has yet to patch this vulnerability.

First Seen in the Wild in Japan

Late this last summer (2013), security researchers began to notice a new Internet Explorer (IE) exploit in Japan. The exploit was first discovered being used against Japanese financial firms on August 29, 2013, though it had probably been around for several months before that. It seemed to only take advantage of Asian (Chinese, Korean, Japanese, Russian) and English language editions of Microsoft products.

It exploits all operating systems, from Windows XP all the way through Windows 8 and Server 2012, using Microsoft's Internet Explorer 7 through 11.

Although there are language restrictions when using Windows XP and Windows Server 2003, there are no language restrictions when exploiting Windows 7 as long as either Microsoft Office 2007 or Office 2010 is installed.

Enables Remote Code Execution

The vulnerability enables remote code execution on a computer that visits a malicious website.

Read: guides on rootkit/listener/meterpreter

The remote code is executed with the same user rights as the Internet Explorer that is being exploited. So, if the user has limited rights on the computer/network, the hacker will come in only with those permissions and then look to escalate their privileges to sysadmin.

If the user has system administrator privileges, well then...it's time to start praying to the computer gods.

Bypasses DEP and ASLR

Interestingly, this new exploit takes advantage of how Internet Explorer handles objects held in memory. It's able to bypass Data Execution Prevention (DEP) and Address Space Layout Randomization (ASLR) by using Microsoft's Office Help Data Services module, enabling it to install its own code for remote execution.

As you know, DEP and ASLR have been implemented in recent years (Linux and Windows in 2004 and Apple in 2006) by nearly every operating system to protect against potential buffer overflow attacks. This once again indicates that NO operating system or application is completely safe.

This vulnerability and exploit is of critical importance as the National Vulnerability Database at NIST rates its severity at 9.3 on a scale of 1 to 10.

Exploit with Metasploit

Then—just about two weeks ago—the Metasploit Project at Rapid7 released an exploit to take advantage of this vulnerability. You can obtain this new exploit by downloading the update to Metasploit. This new exploit can be found among the exploit modules at:

- **exploit/windows/browser/ie_setmousecapture_uaf**

The exploit only takes advantage of this vulnerability on Windows 7 SP1 machines with Office 2007 or Office 2010 installed and Internet Explorer 9. I want to once again emphasize the importance of doing thorough reconnaissance.

Read: guides on active and passive recon

Notice how specific this exploit it is. You must know the operating system, the service pack, the applications, and the browser. It is also important to note that although the exploit in the wild has capabilities to exploit OS's from Windows XP through Windows 8, the exploit developed by Metasploit can ONLY exploit those systems with IE9 on Windows 7 SP1 with Office 2007 or 2010.

They expect to have a more general exploit in the near future.

I will be doing a tutorial on this new exploit and vulnerability in the near future, but I wanted to get it out to our community while it's still hot and unpatched.