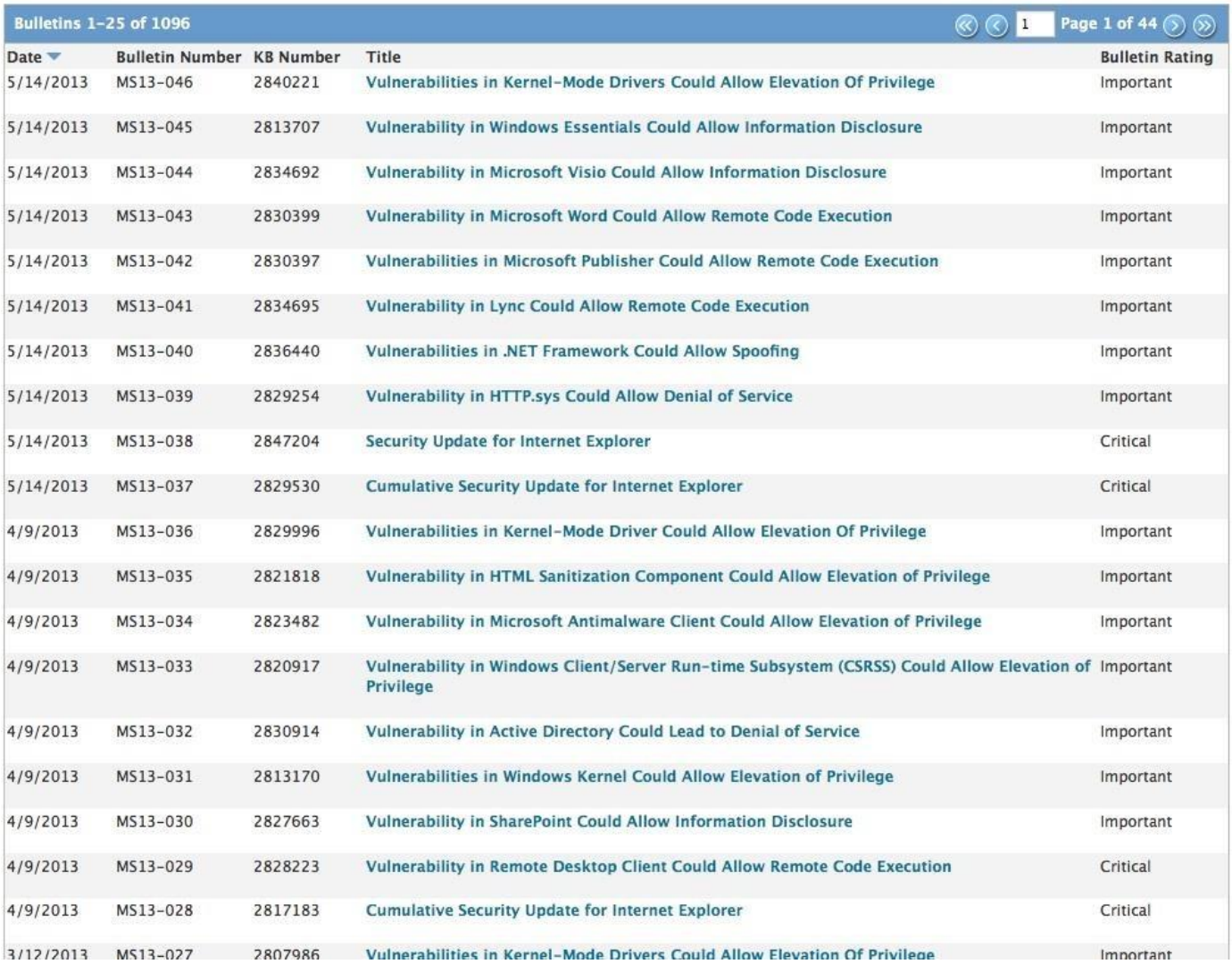
How to Find the Latest Exploits and Vulnerabilities—Directly from Microsoft

Several of you have written me asking about where they can find the latest hacks, exploits, and vulnerabilities. In response, I offer you this first in a series of tutorials on finding hacks, exploits, and vulnerabilities. First up: Microsoft Security Bulletins.

Step 1 Navigate to Microsoft's Technet

As well over 90% of all computers on the planet run a version Microsoft's ubiquitous Windows operating system (although it might surprise you that over 60% of all web servers run some version of Linux/Unix), Microsoft's vulnerabilities obviously are highly valued to the hacker.

Thankfully, Microsoft offers us database of all the vulnerabilities they want to acknowledge, and this can be found at their Microsoft Security Bulletins webpage.



Bulletins 1-25 of 1096 — Page 1 of 44

Date	Bulletin Number	KB Number	Title	Bulletin Rating
5/14/2013	MS13-046	2840221	Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege	Important
5/14/2013	MS13-045	2813707	Vulnerability in Windows Essentials Could Allow Information Disclosure	Important
5/14/2013	MS13-044	2834692	Vulnerability in Microsoft Visio Could Allow Information Disclosure	Important
5/14/2013	MS13-043	2830399	Vulnerability in Microsoft Word Could Allow Remote Code Execution	Important
5/14/2013	MS13-042	2830397	Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution	Important
5/14/2013	MS13-041	2834695	Vulnerability in Lync Could Allow Remote Code Execution	Important
5/14/2013	MS13-040	2836440	Vulnerabilities in .NET Framework Could Allow Spoofing	Important
5/14/2013	MS13-039	2829254	Vulnerability in HTTP.sys Could Allow Denial of Service	Important
5/14/2013	MS13-038	2847204	Security Update for Internet Explorer	Critical
5/14/2013	MS13-037	2829530	Cumulative Security Update for Internet Explorer	Critical
4/9/2013	MS13-036	2829996	Vulnerabilities in Kernel-Mode Driver Could Allow Elevation Of Privilege	Important
4/9/2013	MS13-035	2821818	Vulnerability in HTML Sanitization Component Could Allow Elevation of Privilege	Important
4/9/2013	MS13-034	2823482	Vulnerability in Microsoft Antimalware Client Could Allow Elevation of Privilege	Important
4/9/2013	MS13-033	2820917	Vulnerability in Windows Client/Server Run-time Subsystem (CSRSS) Could Allow Elevation of Privilege	Important
4/9/2013	MS13-032	2830914	Vulnerability in Active Directory Could Lead to Denial of Service	Important
4/9/2013	MS13-031	2813170	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	Important
4/9/2013	MS13-030	2827663	Vulnerability in SharePoint Could Allow Information Disclosure	Important
4/9/2013	MS13-029	2828223	Vulnerability in Remote Desktop Client Could Allow Remote Code Execution	Critical
4/9/2013	MS13-028	2817183	Cumulative Security Update for Internet Explorer	Critical
3/12/2013	MS13-027	2807986	Vulnerabilities in Kernel-Mode Drivers Could Allow Elevation Of Privilege	Important

Here, Microsoft lays out all the details of the vulnerabilities that they are aware of in their operating system and application software. It goes without saying—I think—that zero day vulnerabilities and vulnerabilities that Microsoft doesn't want to acknowledge yet, won't be found here. These vulnerabilities are only those that Microsoft is aware of and has a patch developed for.

So, what good is it to the hacker to be aware of vulnerabilities that Microsoft has patched, you might ask (you did ask that, right?). The answer is that not everyone patches.

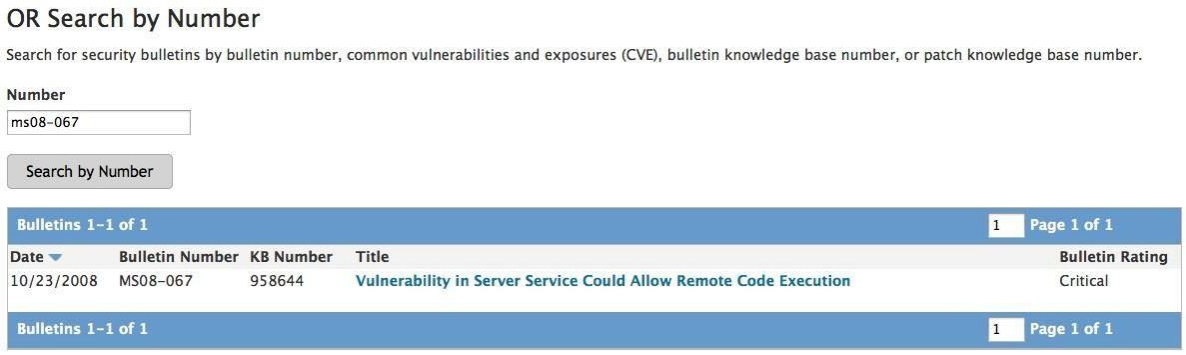
Some users and companies refuse to patch because of the production risks involved and others only patch intermittently. If you check out Netcraft and look up a particular website, it will tell you how long since that website has been re-booted. Generally, a re-boot is necessary to patch a system. If the system has not been re-booted for, say 2 years, we know that all the vulnerabilities listed in Microsoft's security bulletin are available on that

system. When that's the case, you can simply find a vulnerability that has been found within that last two years and then exploit it on that system.

There is also the issue of pirated software. A significant fraction of the world's operating systems and applications are pirated (I'm sure you know at least one person was has pirated software, right?). It is estimated that a majority of the software in China and other developing nations is pirated. This means that these systems will NOT get the latest patches and are vulnerable to the listed vulnerabilities in Microsoft's security bulletins. How nice!

Step 2 Search the Database by Microsoft Vulnerability Number

The Microsoft security bulletins are an easily searched database. You can search it by product, date range or security bulletin number. If you go back and look at some of my Metasploit tutorials, you will notice that I've used an exploit in Metasploit many, many times that's named ms08_067_netapi. That number is the Microsoft security bulletin number. The **ms** stands for Microsoft, of course, the **08** stands for the year the vulnerability was unveiled, 2008, and the 067 means it was 67th vulnerability acknowledged by Microsoft that year. If we search Microsoft's security bulletins for that vulnerability, this is what we find.



Notice that this vulnerability is named "Vulnerability in Server Service Could allow Remote Code Execution". Remote code execution is exactly what we are looking for. It allows listeners/rootkits to be installed and executed remotely. This obviously includes our rootkit of choice, Metasploit's meterpreter. When we click on it, we get the complete report.

Microsoft Security Bulletin MS08-067 - Critical

Vulnerability in Server Service Could Allow Remote Code Execution (958644)

Published: Thursday, October 23, 2008

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in the Server service. The vulnerability could allow remote code execution if an affected system received a specially crafted RPC request. On Microsoft Windows 2000, Windows XP, and Windows Server 2003 systems, an attacker could exploit this vulnerability without authentication to run arbitrary code. It is possible that this vulnerability could be used in the crafting of a wormable exploit. Firewall best practices and standard default firewall configurations can help protect network resources from attacks that originate outside the enterprise perimeter.

This security update is rated Critical for all supported editions of Microsoft Windows 2000, Windows XP, Windows Server 2003, and rated Important for all supported editions of Windows Vista and Windows Server 2008. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by correcting the way that the Server service handles RPC requests. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection for the specific vulnerability entry under the next section, **Vulnerability Information**.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

Top of section

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 2	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 3	Remote Code Execution	Critical	None
Windows XP Professional x64 Edition	Remote Code Execution	Critical	MS06-040

We can see that Microsoft provides us (thank you, Bill!) will an executive summary of the exploit and tells which of their systems are vulnerable. If we page down we can see a list of all affected files and operating systems.

Affected and Non-Affected Software

The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 2	Remote Code Execution	Critical	MS06-040
Windows XP Service Pack 3	Remote Code Execution	Critical	None
Windows XP Professional x64 Edition	Remote Code Execution	Critical	MS06-040
Windows XP Professional x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 Service Pack 1	Remote Code Execution	Critical	MS06-040
Windows Server 2003 Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 x64 Edition	Remote Code Execution	Critical	MS06-040
Windows Server 2003 x64 Edition Service Pack 2	Remote Code Execution	Critical	None
Windows Server 2003 with SP1 for Itanium-based Systems	Remote Code Execution	Critical	MS06-040
Windows Server 2003 with SP2 for Itanium-based Systems	Remote Code Execution	Critical	None
Windows Vista and Windows Vista Service Pack 1	Remote Code Execution	Important	None
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1	Remote Code Execution	Important	None
Windows Server 2008 for 32-bit Systems*	Remote Code Execution	Important	None
Windows Server 2008 for x64-based Systems*	Remote Code Execution	Important	None
Windows Server 2008 for Itanium-based Systems	Remote Code Execution	Important	None

***Windows Server 2008 server core installation affected.** For supported editions of Windows Server 2008, this update applies, with the same severity rating, whether or not Windows Server 2008 was installed using the Server Core installation option. For more information on this installation option, see Server Core. Note that the Server Core installation option does not apply to certain editions of Windows Server 2008; see Compare Server Core Installation Options.

Step 3 Search Vulnerabilities by Product

If we are looking for vulnerabilities in a particular product, we can use this database and search by product. For instance, if I was looking for a vulnerability in Microsoft's Lync (this is Microsoft's enterprise-level instant messaging, VOIP, and video conferencing server with special security features), I can simply select Lync and this database will show me all the vulnerabilities of that product. Here's the most recent vulnerability found in Microsoft's Lync product that "allows for remote code execution" Yeah!

Microsoft Security Bulletin MS13-041 - Important

Vulnerability in Lync Could Allow Remote Code Execution (2834695)

Published: Tuesday, May 14, 2013

Version: 1.0

General Information

Executive Summary

This security update resolves a privately reported vulnerability in Microsoft Lync. The vulnerability could allow remote code execution if an attacker shares specially crafted content, such as a file or program, as a presentation in Lync or Communicator and then convinces a user to accept an invitation to view or share the presentable content. In all cases, an attacker would have no way to force users to view or share the attacker-controlled file or program. Instead, an attacker would have to convince users to take action, typically by getting them to accept an invitation in Lync or Communicator to view or share the presentable content.

This security update is rated Important for supported editions of Microsoft Communicator 2007 R2, Microsoft Lync 2010, Microsoft Lync 2010 Attendee, and Microsoft Lync Server 2013. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by modifying the way that the Lync and Communicator clients handle objects in memory. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection under the next section, **Vulnerability Information**.

Recommendation. Customers can configure automatic updating to check online for updates from Microsoft Update by using the Microsoft Update service. Customers who have automatic updating enabled and configured to check online for updates from Microsoft Update typically will not need to take any action because this security update will be downloaded and installed automatically. Customers who have not enabled automatic updating need to check for updates from Microsoft Update and install this update manually. For information about specific configuration options in automatic updating in supported editions of Windows XP and Windows Server 2003, see Microsoft Knowledge Base Article 294871. For information about automatic updating in supported editions of Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, see Understanding Windows automatic updating.

For administrators and enterprise installations, or end users who want to install this security update manually, Microsoft recommends that customers apply the update at the earliest opportunity using update management software, or by checking for updates using the Microsoft Update service.

See also the section, **Detection and Deployment Tools and Guidance**, later in this bulletin.

↑ Top of section

Knowledge Base Article

Knowledge Base Article	2834695
File information	Yes
SHA1/SHA2 hashes	Yes
Known issues	Yes