[How to Find the Latest Exploits and Vulnerabilities—Directly from Microsoft](https://null-byte.wonderhowto.com/how-to/hack-like-pro-find-latest-exploits-and-vulnerabilities-directly-from-microsoft-0147354/)

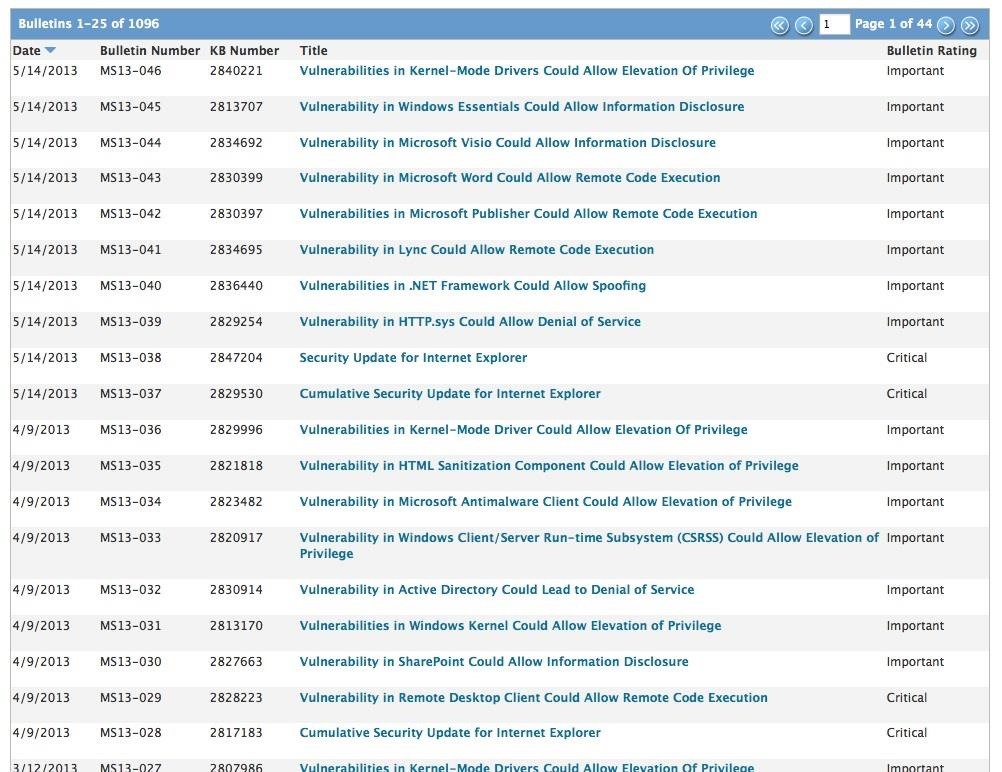
By [**occupytheweb**](https://creator.wonderhowto.com/occupythewebotw/) 06/13/2013 9:32 pm

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](http://technet.microsoft.com/en-us/security/bulletin) webpage.



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.

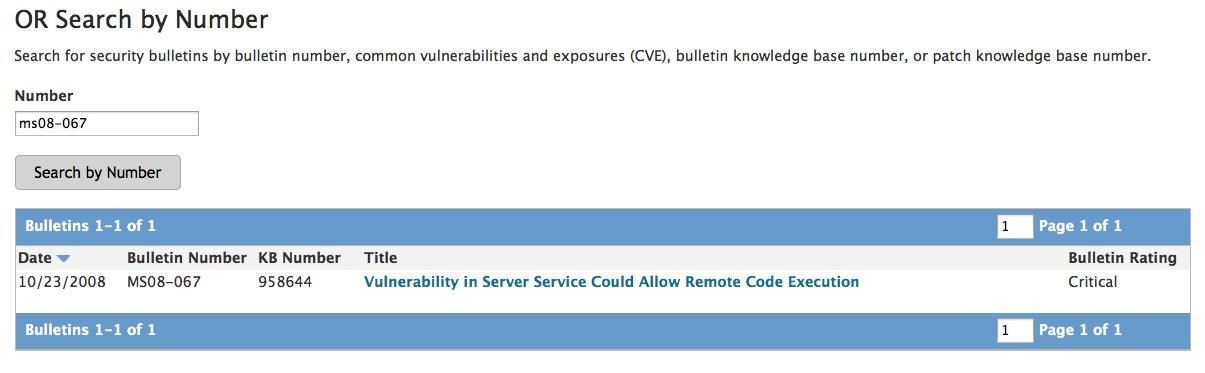
So, what good is it to the hacker to be aware of vulnerabilities that Microsoft has patched, you might ask (you did ask that, right?). The answer is that not everyone patches.

Some users and companies refuse to patch because of the production risks involved and others only patch intermittently. If you check out [Netcraft](https://null-byte.wonderhowto.com/how-to/hack-like-pro-conduct-passive-reconnaissance-potential-target-0146938/) 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.

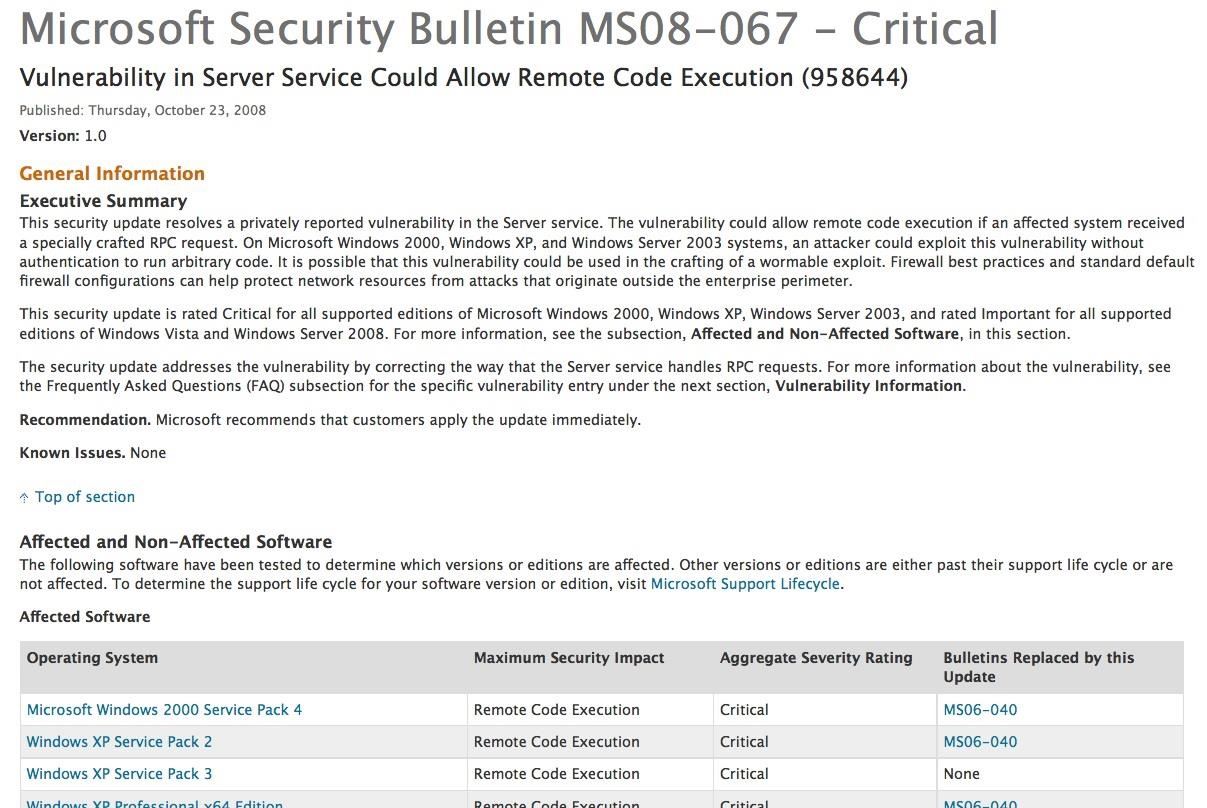
There is also the issue of pirated software. A significant fraction of the world's operating systems and applications are pirated (I'm sure you know at least one person was has pirated software, right?). It is estimated that a majority of the software in China and other developing nations is pirated. 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

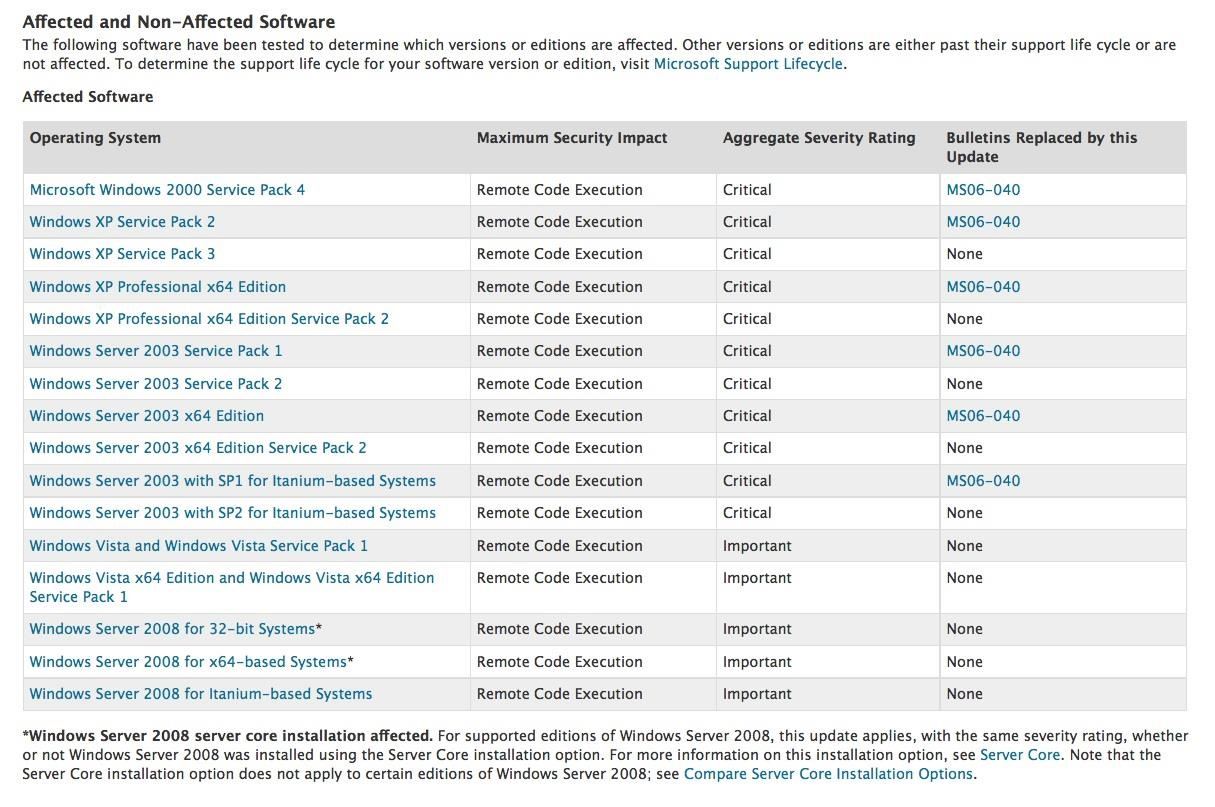
The Microsoft security bulletins are an easily searched database. You can search it by product, date range or security bulletin number. If you go back and look at [some of my Metasploit tutorials](https://creator.wonderhowto.com/occupythewebotw/articles-posted/), you will notice that I've used an exploit in Metasploit [many](https://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-so-you-arent-detected-0146318/), [many](https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-grab-encrypted-passwords-from-compromised-computer-0146655/) [times](https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-grab-screenshot-someones-compromised-computer-0146570/) 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.



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.



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!

