Still using Windows 7? This is the reason security should upgrade to Windows 10

Windows 7 is about to be killed and it will no longer receive software updates. It's time to consider upgrading to a newer operating system.

According to Microsoft, on January 14, 2020, Windows 7 will officially be 'declared dead' and on March 14, 2020, the operating system will no longer receive software updates. It's time to consider upgrading to a newer operating system. Here are the security reasons you should consider upgrading to Windows 10.

1. Instructions to upgrade to Windows 10 from Windows 7/8 / 8.1
2. How to update Windows 10 to the latest version
3. How to install and use Windows 10 without a product key

What is the biggest security issue with Windows 7?

Let's first look at some of the important issues facing Windows 7 users, which will improve when upgrading.

1. The latest Service Pack (Service Pack) for Windows 7 has been Service Pack 1 since 2011. To update Windows 7 requires deploying hundreds of security updates.

2. On Windows 7, Mimikatz and other malicious threats can read the password and other login information from the Local Security Authority Subsystem (LSASS).

3. On Windows 7, anti-virus software must use the API hooking technique to identify some types of malicious activities. This method is less reliable and may not control all hacker attacks.

4. On Windows 7, the popular SmartScreen service is only used in Internet Explorer and does not provide protection for files downloaded by other media.

1. How to scan virus files downloaded on Chrome

5. Windows 7 does not use the TLS 1.2 protocol for WinInet and WinHTTP by default. This is the manual configuration that an administrator needs to know to perform even if they have installed the latest patches.

6. Windows 7 does not support the newer TLS 1.3 protocol. The vulnerabilities in TLS v2 and previous versions are clearly recorded.

Is Windows 10 safer against malware?

Windows 10 offers tremendous improvements in anti-malware protection measures, enhancement of root protection tools and third-party solutions.

7. Windows 10 supports UEFI Secure Boot and Trusted Boot. These options can protect against malicious bootkit running during the boot process and try to "escape" from antimalware tools.

1. Remove root malware (malware) on Windows 10 computers

8. Windows 10 supports Early Launch Anti-Malware, which allows anti-antimalware software to block malicious boot drivers during loading into the system.

9. Windows 10 supports additional LSA protection, allowing the LSASS system to run as a protected process, protecting the login information it stores from malware without the need for a kernel mode component. malicious behavior (kernel mode).

10. Windows 10 supports Protected Anti-Malware Services. Antimalware can run as a protected process, making malicious code more difficult to stop, inject code or tamper with it, even when running with administrative rights.

1. What is Code Injection on Windows?

11. Windows 10 antimalware service provider contains information that helps identify security threats to improve malware detection.

12. Windows 10 integrates a well-known SmartScreen service to check downloads and prevent users from running it if it detects a potential threat.

Which new operating system protection measures does Windows 10 provide?

Many security issues arise from vulnerabilities in the operating system kernel. Windows 10 enhances the protection of the operating system kernel in many different ways and prevents attackers.

13. Windows 10 supports Virtualization Based Security (VBS) and Code Integrity Hypervisor (HVCI). In this mode, the operating system running in a virtual machine and virtual machine monitoring software ensures all operating system kernel mode codes are signed with the correct number. This feature provides strong protection against security and zero-day vulnerabilities trying to run shellcode in the operating system kernel (shellcode is a small piece of machine code that allows you to perform certain tasks within the program. exploited) like NSA's ETERNALBLUE.

14. When turning on VBS, Windows 10 supports Credential Guard, providing a higher level of login protection when running LSA as a protected process. Credential Guard will store login information outside the virtual machine running the operating system. This provides protection to prevent malware from stealing login information even if it successfully downloads a malicious operating system kernel driver.

15. When VBS is enabled, CFG protection is also available for operating system kernel mode codes.

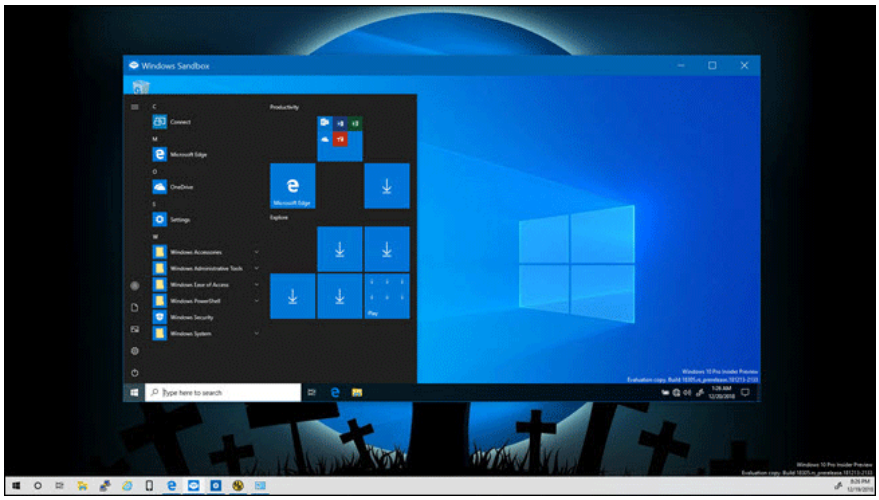
16. Windows 10 enhances the security of the heap and kernel pool, used to allocate dynamic memory in kernel mode and user mode, with different measures making it more difficult to exploit a heap-based vulnerability. .

17. Windows 10 supports process protection policies. Specific programs may choose to participate in these policies to limit code that can run in the process.

18. Previously, the operating system kernel mode component of the Windows GUI subsystem (Win32.sys) was the source of many zero vulnerabilities that malicious software often exploited. Recently an attack on Google Chrome exploited the Win32k vulnerability. Windows 10 introduced more in-depth protection measures for Wind32k, making it more difficult to exploit the vulnerability.

How does Windows 10 enhance the Sandbox feature?

The malicious code is less harmful or even harmless if it is in the sandbox environment. This is more Windows 10 than Windows 7.



19. Windows 10 supports AppContainer technology for sandbox. This feature is mainly used for Windows Store applications but it is also used to handle Untrusted Fonts from operating system kernel mode into the AppContainer environment sandboxed (fontdrvhost.exe) so that malicious fonts do not cause Harmful to the machine.

1. How to configure Windows Sandbox on Windows 10

20. Windows 10 upgrade EMET (Microsoft vulnerability security toolkit) by adding Exploit Guard as part of the system. Administrators can configure to block a specific no-load module process from network sharing and protection against vulnerability exploitation based on ROP (Return Oriented Programming).

21. In addition, antimalware software can use AppContainer technology to sandbox its components when accessing untrusted content. Example: DFI of SentinelOne uses AppContainer on Windows 10.

Is Windows 10 more difficult to penetrate than Windows 7?

Windows 10 supports a number of measures to reduce the exploitation of security vulnerabilities more than Windows 7, helping to protect against zero day vulnerabilities operating on previous Windows operating systems.

21. Windows 10 supports High Entropy ASLR (Address Space Layout Randomization), making the exploit shellcode more difficult to find the code needed for the operation from module download.

23. Windows 10 supports the Control Flow Guard memory protection mechanism. This mechanism makes it more difficult to exploit memory vulnerabilities.

24. Windows 10 supports Code Integrity Guard. The CIG only allows a process with a Microsoft digital signature to be loaded. In addition to use in the Microsoft Edge browser, this policy is used by many system processes in Windows 10 by default, protecting them from being exploited by injecting code from malware.

25. Windows 10 supports Arbitrary Code Guard. ACG allows a process that requires code to originate from the module file (DLL or EXE) and cannot be dynamically allocated, because the vulnerability exploit code usually does so.

26. Windows 10 upgraded BitLocker's protection measures against physical attacks.

Will Windows 10 improve network security?

Network connections from remote login to processing credit card transactions will receive increased security when you upgrade to Windows 10.

27. Windows 10 provides advanced security in Remote Desktop sessions with Remote Credential Guard (RCG). Login information will not be sent to remote servers and protected from attackers on remote servers. RCG also supports Single-Sign-On to enhance password protection.

28. Remote Credential Guard prevents RDP attacks Pass-the-Hash and uses login information after the remote session ends.

29. In Windows 10, Schannel (Windows TLS stack) uses modern TLS protocol versions by default, enhancing security and enabling PCI DSS compliance.

Patch is still a problem on Windows 10?

Say goodbye to Service Pack updates when Microsoft releases Windows 10 updates twice a year and patches released monthly.

30. Windows 10 is always up to date and regular patches are delivered to users monthly so you can be assured of its security.

31. Windows 10 follows the "Windows as a Service" model, providing various service options to enhance security, provide new functions and meet the needs of businesses.

32. In Windows 10, quick service options bring good security measures.

Windows 7 was released 10 years ago, it does not support the latest Intel and AMD processors and when support for Windows 7 ends in March, it will no longer be updated security.

While threats are on the rise, patching is still one of the important ways to deal with security vulnerabilities. Businesses are in the process of transitioning to Windows 10, they will soon receive the security benefits listed

above. And you?

You finished reading the article "**Still using Windows 7? This is the reason security should upgrade to Windows 10**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
