

This video shows exactly why you should not run versions of Windows that are no longer supported

Youtuber with the nickname Eric Parker recently posted a video testing how Windows XP will work in 2024.

This week, Microsoft released a series of Patch Tuesday updates for Windows 10 (KB5037768 / KB5037765 / KB5037763 / KB5037788) and Windows 11 (KB5037771 / KB5037770) scheduled for May 2024. These updates mainly focus on improving Improve the security of the Windows operating system. That is, for Windows versions that are still supported, users can rest assured in terms of security because patches will be released periodically and regularly.

Back when Windows 11 was introduced, Microsoft explained why certain features like TPM 2.0 and VBS were important security requirements, and also illustrated a hacked attack. block thanks to those features.

However, habits as well as reluctance to upgrade and laziness to change make many people tend to look back at the old, discontinued Windows operating system through rose-colored glasses and continue to use them until the end. now despite dozens of security risks the same outdated experience.

Youtuber with the nickname Eric Parker recently posted a video testing how Windows XP, which received its last update 10 years ago, will work in 2024. At the same time, he also pointed out the main update. Exactly why users should not run versions of Windows that are no longer supported.

In the YouTube video above, Eric Parker ran Windows XP in a vulnerable state by disabling Firewall and Defender. As a result, within just a few minutes, suspicious activity was recorded. Malware began to infiltrate the system, and after two hours, the amount of malicious code had increased significantly on the PC.

When delving into malware analysis, this Youtuber found several malicious files trying to operate legitimately. Some of them are labeled Microsoft ("Microsoft compilation" to be precise, not Microsoft Corporation) and others Google. Notably, there is a file that is also named svchost.exe to fool potential victims.

Eric Parker then installed Malwarebytes security software, scanned this Windows XP PC and detected a total of 8 malicious files. As you can see in the image below, they are mainly classified as trojans, adware, and backdoor malware.

Tests like these show how Windows security has improved over time. Even a PC running Windows 11 or 10 without a firewall and antivirus software will not be immediately attacked by various types of malware. As for Windows versions that are no longer supported, the security risk is extremely large.

You finished reading the article "**This video shows exactly why you should not run versions of Windows that are no longer supported**" 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.
