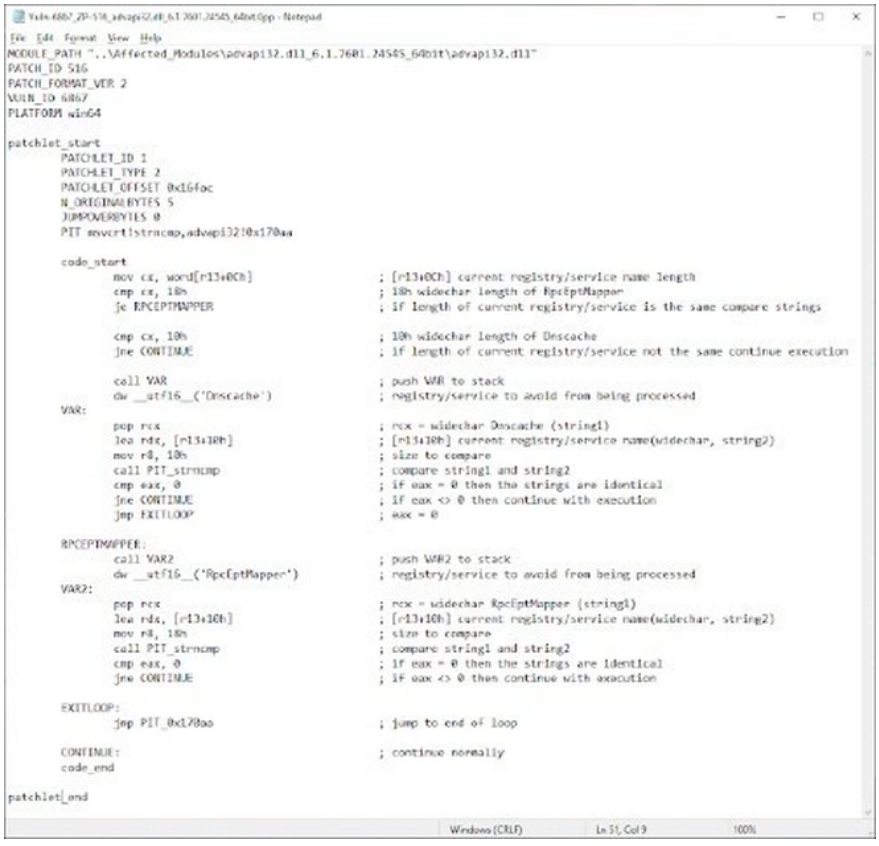
Security vulnerability discovered on Windows 7, affecting millions of users

A security hole has just been discovered in Windows 7 that can affect millions of users. Security researchers recently found a local privilege vulnerability in Windows 7 that could affect millions of Windows users who haven't updated since this release.

Discovered in November, this vulnerability also exists in Windows Server 2008 R2 and Windows 10. Devices running either version of Windows are vulnerable.

According to security researchers, an exploited vulnerability can be extremely serious. While it is not as vulnerable to exploitation as other vulnerabilities found in the system, with an understanding of Windows 7, an attacker can alter the Performance Monitoring System with the privileges that the vulnerability provides. allows the attacker to execute any selected code.



A critical security hole that exists on Windows 7 has just been discovered

In a nutshell, this security vulnerability can affect the user's privacy and resources to the fullest extent when fully exploited, with write access to the following registry keys:

HKLM SYSTEM CurrentControlSet Services Dnscache

HKLM SYSTEM CurrentControlSet Services RpcEptMapper

The bigger problem is that the Microsoft team won't do much to help endangered users. Since Microsoft has moved into the era of Windows 10 and its updates, Windows 7 users will not see any solutions made by Microsoft to this important issue. This has left millions of people dependent on third-party solutions or complete upgrades from the OS.

Fortunately, a cybersecurity company called 0patch has helped users get rid of the dangers of this vulnerability. Users using the affected versions can download it for free at here .