CMC warns the new Trojan

A serious vulnerability in Windows Shell was discovered on July 15 and is currently being exploited by Stuxnet malicious code.

A serious vulnerability in Windows Shell was discovered on July 15 and is currently being exploited by Stuxnet malware, while Microsoft has yet to release a patch .

However, users can be assured because the anti-virus versions of CMC Internet Security / CMC Antivirus have detected and killed the Trojan variants that take advantage of this security hole.

This vulnerability was exploited by hackers to execute malicious code with the aim of taking full control of the user's system. After successful occupation, they will install malicious programs, change or delete data. It is worth mentioning here that just if the user plugs the USB into the computer which contains the .Ink file (shortcut format) that has been embedded the malicious code, the malicious file will be executed as soon as the user clicks on the USB. The danger of this vulnerability is that the virus can automatically activate even if the user has disabled AutoPlay and AutoRun.

Windows versions affected by this error include : Windows XP SP3, XP Pro x64 SP2, Windows Server 2003 SP2, Server 2003 x64 Edition SP2, Vista SP1 / SP2, Vista x64 SP1 / SP2, Windows Server 2008 / SP2 and x64 / SP2, Windows 7 32-bit and 64-bit, Windows Server 2008 R2 64-bit.

CMC InfoSec security experts recommend users to use USB scanning antivirus software before performing any operation, and should monitor and update the patch as soon as Microsoft offers.

You finished reading the article "**CMC warns the new Trojan**" 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.
