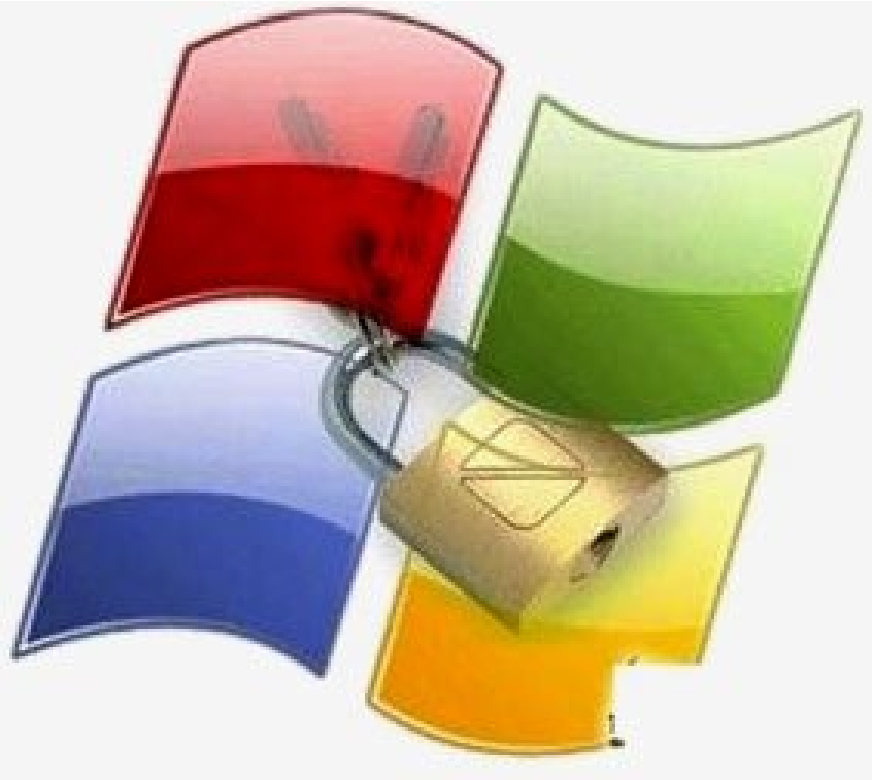
Trojan attacks on dangerous errors in Windows

An unpatched vulnerability in Windows has been confirmed by Microsoft that could be exploited by hackers to take control of the new 'favored' trojan system.

An unpatched vulnerability in Windows has been confirmed by Microsoft that could be exploited by hackers to take control of the new " *favor* " trojan system.



Microsoft has officially terminated technical support for Windows XP SP2 on July 13, similar to the Windows Vista version on April 13, 2010. Therefore, the newly discovered vulnerability threatens Windows XP SP2 users may not be patched by Microsoft, instead the software company recommends that users upgrade immediately to Windows XP SP3 to be able to update patch when it is released.
Microsoft is still supporting Windows operating system versions including: Windows XP SP3, Vista, Server 2003, Windows 7, Server 2008, Server 2008 R2 and even upcoming beta versions of Windows 7 SP1 and Server 2008 R2 SP1.

Dangerous errors are in the "shortcut" files (* .lnk format) of Windows, these files are usually located on the desktop or Start menu interface. The attacker will use a USB storage device containing a " **shortcut** " file that has been embedded in the malicious code on the user's computer. If the victim views the content on the USB

flash drive with file managers such as Windows Explorer, the system will be taken over.

In addition, the error can also be exploited remotely via USB flash drive. The "shortcut" files embedded with malicious code can be distributed over the internet.

- Error code: **2286198**

- Windows versions are affected by errors: 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.

- Patch: not yet released

According to *Dave Forstrom* , director of Trustworthy Computing group of Microsoft said the error is being exploited by **Stuxnet** malicious code. The Microsoft team has discovered more than 6,000 plots to infect Windows XP SP2-based computers since July 15. **Stuxnet contains a type of trojan that downloads remote attack code including rootkits hidden in the system** .

Chester Wisniewski , a senior security expert at Sophos, said the error could be successfully exploited even if two **AutoRun** and **AutoPlay** functions (self-activating content on the drive) were locked. Rootkits will bypass Windows' security check system including UAC found in Windows Vista and Windows 7 (UAC - User Account Control, the action confirmation window will usually appear every time an user performs an operation. on Windows).

Microsoft has not officially announced the release date of the patch. Windows users may have to wait for a regular patch on August 10.

How to prevent temporary errors

Users are advised by Microsoft to **temporarily lock the shortcut display function** and turn off the **WebClient** service until an official patch is available. Since locking the display of the shortcut must be done in the Registry system, it may cause problems for Windows so readers need to back up the registry before proceeding.

To lock the shortcut file, do the following:

- **Go to Start** , **Run** , type **regedit** and **Enter** to open the **Registry** system.

- Find the value key: **HKEY_CLASSES_ROOTlnkfileshellexIconHandler** , click the **File** menu and select **Export** .

- In the **Export Registry File** dialog box, enter the name **LNK_Icon_Backup.reg** and click **Save** . The backup file will be put in the **My Documents folder** .

- Select the value (**Default**) in the right pane of **Registry Editor** , press **Enter** to change the value. You remove the value, leave it blank and press Enter to confirm the change.

Exit **Registry Editor** , restart the computer to execute the changes. Your desktop will lose shortcut files.

To turn off the WebClient service, type **Services.msc** in the **Start** - **Run** dialog box and click **OK** . Must select on WebClient, click **Stop** to stop if this service is active or **Disabled** to lock.

After updating the patch, you can restore the registry and reactivate the WebClient service.

You finished reading the article "**Trojan attacks on dangerous errors in Windows**" 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.
