

IT Security: Microsoft admit to serious security problem in Windows Shell.

Microsoft has issued a warning that it has identified a serious flaw in the shell of its Windows operating system - it affects almost all computers running the Windows operating system where removable drives are used. That includes all sticks, hard disks and other devices running via USB ports.

The Microsoft announcement says "The vulnerability exists because Windows incorrectly parses shortcuts in such a way that malicious code may be executed when the icon of a specially crafted shortcut is displayed. This vulnerability is most likely to be exploited through removable drives. For systems that have AutoPlay disabled, customers would need to manually browse to the affected folder of the removable disk in order for the vulnerability to be exploited. For Windows 7 systems, AutoPlay functionality for removable disks is automatically disabled. Microsoft is currently working to develop a security update for Windows to address this vulnerability."

Systems such as XP automatically run drives when they are plugged in. The potential for viruses and other malware to run from a stick is well known. F-Secure says that simply loading the disk would be sufficient for some malware to load onto the PC and run.

The "exploit," as such things are known, uses a rootkit called "Stuxnet" - which is able to hide files with two characteristics: file type .lnk and files that start ~WTR and having file type .tmp.

For users, there is an added complication: by default, Windows hides the file-type extension. It also hides files starting with ~.

Lumension Security says, on its blog, that the malware dives under the autorun facility and therefore simply turning that off will not work. It also - in ways not so far understood - is not picked up by antivirus programs - and gets out through firewalls.

Stuxnet modifies Windows' basic browser software, iexplore.exe. Because users - and indeed Windows default settings - approve Internet Explorer to pass through firewalls. Some researchers also report that Stuxnet has tools built into it which enable it to shut down some security software.

Microsoft says that is working to build a fix for the problem which affects Windows XP, Vista and 7. It may also affect previous versions of Windows but Microsoft does not support them and so ignores the possible risks to users.

Microsoft suggests some "workarounds" as a temporary measure. But those involve modifying the Registry - a task best left to those with nerves of steel and deep understanding of the innards of Windows - and disabling the web-client service, a step that involves accessing the Windows DOS window, a place many SysOps would rather the staff in their company did not know about.