

Microsoft: 'Đừng nhấn phím F1 trong Windows XP'

Tập đoàn phần mềm Mỹ khuyên người dùng không nên nhấn phím trợ giúp (F1) khi một website nào đó "gợi ý" vì họ có thể rơi vào bẫy của hacker.

Microsoft vừa thừa nhận một lỗ hổng trong VBScript mà chuyên gia người Ba Lan Maurycy Prodeus phát hiện tuần trước có thể tạo điều kiện cho hacker khống chế máy tính cài Internet Explorer (IE).

"Lỗ hổng này tương tác với các file Windows Help khi sử dụng Internet Explorer. Cho đến khi bản vá lỗi sẵn sàng (thời gian chưa xác định), người dùng nên tránh bấm F1 khi một website yêu cầu, hoặc khóa hệ thống Windows Help", đại diện Microsoft cho hay.

Sự cố ảnh hưởng đến Windows 2000, Windows XP và Windows Server 2003 trong khi các hệ thống Windows Vista, Windows Server 2008, Windows 7 và Windows Server 2008 R2 vẫn an toàn.

Châu An (theo ComputerWorld)

Don't press F1 key in Windows XP

March 1, 2010

Computerworld - Microsoft told Windows XP users today not to press the F1 key when prompted by a Web site, as part of its reaction to an unpatched vulnerability that hackers could exploit to hijack PCs running Internet Explorer (IE).

In a security advisory issued late Monday, Microsoft confirmed the unpatched bug in VBScript that Polish researcher Maurycy Prodeus had revealed Friday, offered more information on the flaw and provided some advice on how to protect PCs until a patch shipped.

"The vulnerability exists in the way that VBScript interacts with Windows Help files when using Internet Explorer," read the advisory. "If a malicious Web site displayed a specially crafted dialog box and a user pressed the F1 key, arbitrary code could be executed in the security context of the currently logged-on user."

Last week, Prodeus called the bug a "logic flaw," and said attackers could exploit it by feeding users malicious code disguised as a Windows help file -- such files have a ".hlp" extension -- then convincing them to press the F1 key when a pop-up appeared. He rated the vulnerability as "medium" because of the required user interaction.

Windows 2000, Windows XP and Windows Server 2003 are impacted by the bug, said Microsoft, and any supported versions of Internet Explorer (IE) on those operating systems -- including IE6 on Windows XP -- could be leveraged by attackers. Previously, Prodeus had said that users running IE7 and IE8 were at risk, but had not called out IE6.

Until a patch is ready, users can protect themselves by not pressing the F1 key if a Web site tells them to, said Microsoft.

"As an interim workaround, users are advised to avoid pressing F1 on dialogs presented from Web pages or other Internet content," said David Ross with the Microsoft Security Response Center (MSRC) engineering staff in a blog entry on Monday.

"The prompt can appear repeatedly when dismissed, nagging the user to press the F1 key," Ross added.

The security advisory made the same recommendation: "Our analysis shows that if users do not press the F1 key on their keyboard, the vulnerability cannot be exploited."

Users can also stymie attacks by disabling Windows Help. The advisory explained how to entering a one-line command at a Windows command-line prompt to lock down the Help system.

The company took Prodeus to task for taking the bug public, something it regularly does when researchers disclose a vulnerability or post sample attack code before a patch is available.

"Microsoft is concerned that this vulnerability was not responsibly disclosed, potentially putting customers at risk," said Jerry Bryant, a senior manager with the MSRC, in an e-mail. By Prodeus' account, he notified Microsoft of the flaw Feb. 1, about four weeks before publishing his findings. Microsoft has not set a timeline for a fix, saying only that, "Microsoft will take the appropriate action to help protect our customers." The next scheduled security patch date for the company is March 9.

Although it does not rate the severity of vulnerabilities in its advisories, Microsoft noted that hackers exploiting the VBScript flaw using Windows Help and Internet Explorer could grab complete control of a Windows system.

Customers running Windows Vista, Windows Server 2008, Windows 7 or Windows Server 2008 R2 are safe from such attacks, Microsoft said.

http://www.computerworld.com/s/article/9164038/Microsoft_Don_t_press_F1_key_in_Windows_XP