Microsoft patched drive-by errors in March

Microsoft yesterday released three security updates that patch four vulnerabilities in Windows and Office.

TipsMake.com - **Microsoft yesterday released 3 security updates to patch 4 vulnerabilities in Windows and Office. And, as expected, Microsoft did not release a patch for Internet Explorer (IE) to create an opportunity for the Pwn2Own contest, the hack contest will take place today.**

Even the company called this patch a "breathless" phase for users. Jerry Bryant, head of Microsoft Security Response Center (MSRC), a team in charge of investigating, patching and resolving problems, said: ' *This is a mild month* .'

Microsoft seems to be accustomed to the habit of providing fewer patches in the odd month. For example, in January, they only provided 3 patches while the previous month provided 22 patches.

One of the 3 patches provided - Microsoft calls them bulletins - rated 'serious', the firm's highest danger. The remaining 2 copies are considered 'important', the second highest level of warning.

Bulletin MS11-015 is the only serious update patch.

Wolfgang Kandek, CTO of Qualys, said: ' *This is the patch we are most interested in* .'

This update patches a pair of vulnerabilities, including one of Windows Media Center and Windows Media Player found in nearly all versions of Windows. This vulnerability 'resides' in Digital Video Recording files (DVR-MS), created by the Stream Buffer Engine (SBE) tool and stored with ".dvr-ms" file extension.

When it comes to this type of attack, it can be exploited simply by persuading users to access malicious code sites, Bryant said. " *This is a browsing and browsing vulnerability* ."

Andrew Storms, director of security operations at nCircle Security said: ' *This is a drive-by vulnerability. There are two mining methods, first in an IFRAME, a typical drive-by type. The next type is in the form of email attachments, which appear when users frequently open them, not just preview (in their email accounts)* '.

According to Angela Gunn, director of communications for Microsoft MSRC central security, all versions of Windows, including Windows XP, Vista and Windows 7, can be hacked unless patched. The only exception: Windows XP Home Edition because it does not support vulnerable codecs.

The second vulnerability in MS11-015, and two other vulnerabilities patched in MS11-016 and MS11-017, are classified as " **DLL load hijacking** " vulnerabilities, sometimes called " **binary planting** " vulnerabilities - implanted. binary.

Researchers first revealed bugs related to DLL load hijacking issues in Windows and Microsoft software and many third-party Windows applications in August last year. Microsoft started patching **DLL load hijacking** in their software last November.

In December, Bryant said Microsoft believed they could complete the task of **DLL load hijacking** . However, in the past January and February, the company still has problems patching this error.

Yesterday, Bryant said: ' *This will make us continue our investigation. Although we think we have found all of these vulnerabilities in IE, we are still investigating the company's remaining products* . '

Both Kandek and Storm said that Microsoft seems to be able to continue implementing **DLL load hijacking** errors in the near future. Kandek said: ' *This will happen in the next few years and not only will Microsoft do the work that third-party vendors will also do* .'

Although the warning bell has rang since August and Microsoft has quickly provided a tool to block malicious attacks, hackers have not used the technology to harm Windows computers, or if they have use, their efforts are not detected.
This does not surprise Storms.

He said: ' *These gaps are difficult to exploit. Last year, it was easy, but it turned out not to be easy to exploit these vulnerabilities, because it required users to browse to the area containing the malicious code and open the file, and the attackers would Put a malicious* ***DLL*** *and a bad file. That's just a few steps* '.

HD Moore, head of Rapid7's security staff and creator of the Metasploit toolkit open source toolkit, yesterday announced to businesses that they can turn the exploit of any **DLL** vulnerability. Which **hijacking load** becomes more difficult for any hacker by removing WebDAV service on all Windows machines, and blocking outbound ports 139 and 445.

Last year, Moore was one of the first to reveal the new level of **DLL load hijacking** vulnerability **.**

However, Microsoft did not patch IE before the Pwn2Own hack contest took place today.

Pwn2Own, which will put security researchers 'against' four browsers, including Microsoft's IE, Apple's Safari, Google's Chrome and Mozilla's Firefox, will take place from November 9 at the CanSecWest conference in Vancouver. Canada. The first security researcher who defeats IE, Safari or Firefox will receive a $ 15,000 prize,

and anyone who gets off the Chrome browser will receive a $ 20,000 prize.

Yesterday (March 8), Bryant said that customers' patching should not be interrupted with surprising security updates to create opportunities for the Pwn2Own competition.

Bryant said: ' *I don't see any reason to disrupt customers just because of the competition. Going out is a potential interruption, and we won't do this unless a vulnerability is being attacked* . '

Microsoft refused to preempt IE before Pwn2Own was not a surprise: The company provided updates for IE in even months, and the latest browser update was released on August 8. 2 past.

Bryant added, in any case, that any holes exploited at Pwn2Own leaked out were not harmful because the errors discovered at this contest will be reported to the vendor. level discreetly.

HP TippingPoint Group, which owns Zero Day Initiative (ZDI) security research program, generously donated Pwn2Own and paid most cash prizes, acquired ownership of the discovered holes in the competition and awarded Leave them to suppliers. ZDI gives developers six months to patch any vulnerabilities they buy before they publish official information.
Both Google and Mozilla have recently patched their browser - Google patched early yesterday - and Apple is expected to update Safari before Pwn2Own starts.

Microsoft updates can be downloaded and installed via Microsoft Update and Windows Update services, as well as through Windows Server Update Services (WSUS).