

# Microsoft provides security patches for Windows, IE

Yesterday (April 12), Microsoft provided a record patch package, up to 64 patches for Windows, Office, Internet Explorer (IE), and other software, including 30 bugs in Windows and an error in IE.

*TipsMake.com* - Yesterday (April 12), Microsoft provided a record patch package, up to 64 patches for Windows, Office, Internet Explorer (IE), and other software, including 30 bugs in Windows and an error in IE were discovered in the new Pwn2Own hack contest that took place last month.

>>> Patch Tuesday of April 2011 will be very 'terrible'



In addition, the company also provides a 'backdoor' in Office 2003 and Office 2007, bringing one of Office 2010's latest security features into older versions.

17 updates that Microsoft attaches to the name " **bulletins** ", set a record late last year, but easily defeated the October 2010 number by the total number of vulnerabilities they patched. Overall, yesterday's update was 64 holes, 15 more than October and 24 losses compared to last December's patch.

9 out of 17 bulletins are marked 'serious' (the most dangerous level of Microsoft), while the remaining patches are marked 'important' (the second highest danger level).

Microsoft and nearly all security experts mark updates that users should download and install immediately.

Jerry Bryant, head of Microsoft Security Response Center (MSRC), said in an interview: "*There are three patches we think are worth the first priority.*" Bryant marked MS11-018, MS11-019 and MS11-020 as updates that should be downloaded and installed as soon as possible.

MS11-018 patched 5 vulnerabilities in IE, 3 of them were serious, including 1 hole discovered by Stephen Fewer researcher in the Pwn2Own hack contest last month (he left the competition with a valid check \$ 15,000 and a new notebook).

Bryant said: '*We encourage customers to uphold these patches because we have seen targeted attacks using the Pwn2Own vulnerability.*'

Microsoft acknowledged these attacks the other day in a tweet from MSRC.

---

This seems to be that the IE vulnerability exploited in the Pwn2Own contest has somehow been exposed to the outside because others cannot discover this vulnerability in the contest: HP TippingPoint, the sponsor of the event. Exam, do not reveal information about the vulnerabilities they have purchased.

Andrew Storms, director of security operations at nCircle Security, said: '*We still see a lot of people finding a gap.*'

Another bulletin is also on the top of everyone's list of priorities: MS11-020, which fixes a critical flaw in Windows' SMB (Server Message Block) protocol.

Amol Sarwate, Director of Qualys Inc's Security Research Department, said: '*This is a familiar flaw, something we have seen for a long time. There is no need for any user effects to activate, and once infiltrated inside, a worm using this hole can spread through the entire network.*'

Storms, like Sarwate when ranking SMB updates with IE bulletin, indicates that Conficker worm has exploited a serious vulnerability.

Conficker, which began to attack Windows-based computers in November 2008, spread through millions of computers within a few months, and caused a media disturbance in April 2009 when one a large number of computers that received new malware updates, also exploited a SMB vulnerability.

Even when Microsoft rushed to release an emergency patch before Conficker appeared, the worm spread widely and quickly.

Storms said: '*I don't know which version is more important, MS11-018 or MS11-020. However, an SMB error is a kind of vulnerability. It is another Conficker.*'

Suppose an attacker could 'implant' malware on the computer - not difficult when people click on the link without noticing - he can use the patched **SMB** error in **MS11-020** to spread the worm. to another computer on the same network.

Storms said: ' *We have learned a lot of lessons from Conficker, and recommend that people install this patch immediately* '.

**MS11-019** , another patch also focused on the SMB protocol, is Bryant's third update to give top priority.

Besides, the company also released patches for Excel, PowerPoint, .Net and many other small parts of Windows.

In the last section, **MS11-034** patched 30 vulnerabilities in Windows Kernel device drivers. All 30 patches were reported by Tarjei Mandt, a researcher working for Norman ASA, a Norwegian antivirus company.

Microsoft has also released two security advisory versions, which users can retrieve and install.

According to the researchers, the most remarkable thing about these two versions is that they provide a file authentication security feature, which first appeared in Office 2010 with users using Office 2003 office applications and Office 2007.

In December 2010, Microsoft announced that it could add file validation features to Office 2003 and Office 2007, adding that it could do this earlier this year.

Security patches can be downloaded and installed through Microsoft Update and Windows Update services, as well as through Windows Server Update Services.

You finished reading the article "**Microsoft provides security patches for Windows, IE**" 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.