Protect yourself against the new Internet Explorer VML vulnerability

Although Microsoft has confirmed IE's new natural vulnerability is increasingly damaging monsters in the cyber world. But the company is still only committed to making a fix according to its regular monthly plan. Expected new version and bug will be released

Although Microsoft has confirmed IE's new natural vulnerability is increasingly damaging monsters in the cyber world. But the company is still only committed to making a fix according to its regular monthly plan. Expected new version and error will be released on October 10. So, until before the manufacturer's patch, what should users do to protect themselves? You can refer to the following steps.

1. Eliminate the gap '*. dll* ': In the customer security advisory section yesterday, Microsoft recommends that users stop using the' *vgx.dll* 'library with the command line:

regsvr32 / u "% CommonProgramFiles% Microsoft SharedVGXvgx.dll

in the *Run* window (go to *Start*> *Run*> type the command above> *OK*> *OK*).

To restore the use of the library, you can use the command:

regsvr32 "% CommonProgramFiles% Microsoft SharedVGXvgx.dll

2. Use Group Policy to replicate the suspension process. ' *dll* ':

Create a Group Policy object folder to interrupt (or restore) the process of using the '.dll' library for all users in a Windows domain (domain).

3. Remove binary and script activities in IE 6:

Microsoft also offers another secure way to turn off all script components in the browser. But it should be noted that this measure only fights existing known vulnerabilities, and many other vulnerabilities may not work at all.

1. In IE, select *Tools> Internet Options*
2. Click on the ' *Security* ' tab.
3. Click " *Internet* " then " *Custom Level* "
4. In the " *ActiveX controls and plug-ins* " section, under the " *Binary and Script Behaviors* " section, click the " *Disable* " *tab* and click OK.

Repeat the last step above, but in the " *Local intranet* " area.

4. Use another browser:

IE 6 is heavily influenced by zero-day vulnerabilities. And ' *one of the easiest ways is to use Firefox with a plug-in (allow extra features), allow websites (like windowsupdate.com) to use MSIE to return ActiveX functionality. Users do not need to choose or use any other component* '.

Both plug-ins add IE features to Firefox: IE Tab and IE View. In Firefox language they are also called 'extensions'.

In this case, 'other browsers' can also be Internet Explorer 7. Currently IE7 is in Release Candidate 1. According to a Microsoft spokesman on Tuesday, IE 7 does not encounter errors in the VML vulnerability.

You can download IE 7 RC1 at Microsoft's website.

If you want more information about this security error, you can read this article.