Microsoft patched 15 bugs, continued to patch SSL certificates

Microsoft finally released an update patch after 4 days of detailed information leakage.

TipsMake.com - **Microsoft finally released an update patch after 4 days of leaked details.**

The company also added a solution to the DigiNotar hacking by "kill switch" on the SSL (secure socket layer) certificate provided by DigiNotar (CA) security vendor.

However, news about 5 updates or 15 bugs that Microsoft released yesterday is not new: last Friday, the company leaked information about security bulletins, the term Microsoft used. for instructions included with each update.

All updates and vulnerabilities are rated as important, the second highest in the company's rating system.

2 of these vulnerabilities are in Windows; 5 in Excel - spreadsheet included in Office office applications; 2 vulnerabilities in non-Office applications; and the remaining 6 vulnerabilities affect SharePoint and other software, such as Groove and Office Web Apps.

Of the 15 vulnerabilities, there are two " *DLL load hijacking* " vulnerabilities, a term used to describe a type of error that has occurred since August 2010. Microsoft patched its software to solve this problem.

Obviously, this work has not been completed yet because Microsoft has not closed the 2010 consulting channel to warn users about DLL load hijacking vulnerabilities in its software.

According to security experts, the user update should be deployed first MS11-072.

This is a release containing vulnerability patches for all versions of Excel, including Excel 2010 on Windows and Excel 2011 on Mac.

When asked about which update deserves the top spot on the list, Andrew Storms, director of security operations at nCircle Security, said: ' *That is an update to Excel because that is the direction. Public through the file has been changed* '.

Other experts also agree with the above opinion.

Wolfgang Kandek, chief technology officer of Qualys security firm, said: ' *The first priority should be on MS11-072, a patch that will help resolve pseudo executable code in Excel files. It affects all versions of Excel, including the most recent version of Excel 2010. To exploit this problem, hackers will create Excel files that contain malicious code and when opened on vulnerable hosts. , it will gain control of the system* '.

Kurt Baumgartner, Kaspersky Lab's security expert, added: ' *Excel-related attachments and links are often used to attack organizations and it deserves us to be of top concern* '.

Other updates patched in WINS (Windows Internet Name Service), a component of Windows Server that was patched last May; and fix script vulnerabilities in SharePoint Server 2010.

Along with 5 updates, Microsoft provides another update to deal with the theft of more than 500 electronic certificates from DigiNotar (CA) security vendor.

According to Pete Voss, Microsoft Trustworthy Computing group expert, ' *We also released another update, adding 6 original DigiNotar certificates for Untrusted Certificate Store (unsafe certification repository) "* .

DigiNotar's signed certificates are then signed by another CA (in this case Entrust or GTE) to allow them to be used by Windows computers or browsers that are not yet authenticated. DigiNotar.

According to Storms, the certificates issued by Entrust or GTE will not affect this update.

Earlier, Microsoft and its competitors, such as Google, Mozilla or Apple, "competed" to ban or block DigiNotar certificates. September security patches can be downloaded and installed through Microsoft Update and Windows Update services, as well as through Windows Server Update Services.