Microsoft sends security patches, urges fix-it for XML Core Services vulnerability

June 14 2012, by Nancy Owano

(Phys.org) -- Confirm, warn, patch. Microsoft has had a busy week, this being the week of Patch Tuesday, an event held on the second Tuesday of the month, when Microsoft releases security patches. On this latest Patch event, Microsoft issued seven security bulletins, three of which were termed as critical, warning users of twenty-six vulnerabilities in Microsoft products, a number of them involving Internet Explorer. The patches affect supported Windows versions, the .NET Framework, Remote Desktop, Lync and Dynamics AX. A patch that had been announced for Visual Basic for Applications has yet to be released.

MS12-037, especially, is being discussed as a critical bulletin that addresses 13 vulnerabilities in Internet Explorer 6, 7, 8 and 9 that could allow for remote-code execution. Security managers have seen this bulletin as pertinent, as IE is so widely used in homes, businesses and public organizations.

In its IE security update, Microsoft said the most severe vulnerabilities could allow remote code execution if a person uses IE to visit a booby-trapped webpage. The attacker could gain control of the computer with the same user rights as the browser victim. Those especially vulnerable to the exploit are users operating with administrative rights; less so for users whose accounts are configured to have fewer rights.

The security update is rated Critical for IE 6, 7, 8, and 9 on Windows clients. As most customers have enabled automatic updating, the security update will be installed automatically. Customers who have not enabled automatic updating need to install this update manually.

Another advisory in the Patch lineup addresses security weaknesses in Microsoft XML Core Services, again opening the user up to remote code execution. Microsoft said it was still investigating this and plans to issue a solution through its monthly release process or if necessary an out of cycle security update. Meanwhile, Microsoft has issued a "Fix it" solution intended to block the attack vector. Microsoft encourages customers running an affected configuration to apply the Fix it solution as soon as possible. The vulnerability affects all supported versions of Windows and editions of Microsoft Office 2003 and Microsoft Office 2007.

The Microsoft update MS12-036, labeled as Critical, concerns denial of service and remote code execution vulnerabilities in the Remote Desktop features that are built into supported versions of Windows. Microsoft warns that vulnerability in Remote Desktop allows remote code execution. This is when the attacker sends a sequence of crafted RDP packets to an affected system. Those who do not have the RDP enabled on Windows are not at risk. The update will be installed automatically for users whose systems have automatic updating.

More information:
technet.microsoft.com/en-us/se … ty/bulletin/ms12-037
technet.microsoft.com/en-us/se … ity/advisory/2719615
technet.microsoft.com/en-us/se … ty/bulletin/MS12-036
technet.microsoft.com/en-us/se … ty/bulletin/ms12-jun

Citation: Microsoft sends security patches, urges fix-it for XML Core Services vulnerability (2012, June 14) retrieved 10 April 2024 from https://phys.org/news/2012-06-microsoft-hole-patches-urges-fix-it.html