M$ issues 'maximum severity' Windows alert

By *srlinuxx*
Created *11/05/2005 - 5:25pm*
Submitted by srlinuxx on Wednesday 11th of May 2005 05:25:31 PM Filed under Microsoft [1]

Microsoft has warned of a flaw in its Windows operating system that could be exploited by hackers to remotely run malicious applications on a victim's PC.

The Redmond giant explained that the remote code execution vulnerability, which it rates "maximum severity rating: important", concerns the way that Web View in Windows Explorer handles certain HTML characters in preview fields.

"By persuading a user to preview a malicious file, an attacker could execute arbitrary code in the context of the logged on user. The vulnerability is documented in the 'Vulnerability Details' section of this bulletin," Microsoft stated.

The flaw means that, if a user is logged on with administrative rights, an attacker who successfully exploited this vulnerability could take complete control of an affected system.
An attacker could then install programs, view, change or delete data, or create new accounts with full user rights, Microsoft warned.

Users whose accounts are configured to have fewer user rights on the system could be less affected than those who operate with administrative user rights.

Microsoft noted that user interaction is required to exploit the vulnerability, but added that customers need to apply the update "at the earliest opportunity".

According to the software giant's Security Bulletin MS05-024, any user running Windows 2000 Service Pack 3 or Windows 2000 Service Pack 4 should immediately update their systems with the relevant patch.

The company stressed that all versions of Windows XP and Windows Server 2003 are not affected by the flaw, and that Windows 98, Windows 98 Second Edition, and Windows Millennium Edition are not "critically affected" by the bug.

Source.

Microsoft

Links:
[1] http://www.tuxmachines.org/taxonomy/term/62