Hackers probe Outlook Express flaw

By *srlinuxx*
Created *25/06/2005 - 2:44pm*
Submitted by srlinuxx on Saturday 25th of June 2005 02:44:23 PM Filed under Microsoft [1]

The risk of an attack related to a flaw in Microsoft Outlook Express climbed this week, after underground hacking sites began circulating sample code for exploiting it.

The exploit, which the French Security Incident Response Team drew attention to on Monday, is designed to take complete control of PCs with certain versions of the Outlook Express e-mail program installed on them, when users visit newsgroups controlled by the hackers.

But security experts said the risk of a widespread attack is low, because people must visit the malicious newsgroups for an attack to work. In addition, the exploit code that's in circulation has some glitches, said Michael Sutton, a lab director at security company iDefense.

It requires a reasonable amount of user intervention, which lowers the overall risk," Sutton said.

Nonetheless, iDefense urges people with vulnerable machines to install the patch Microsoft released last week to fix the flaw. The problem stems from a component of Outlook's newsreader program called Network News Transfer Protocol. The result of an attack could be serious.

"An attacker could install programs; view, change or delete data; or create new accounts with full user rights," Microsoft warned in a security bulletin for the patch last week. The company rated the vulnerability "important," which falls second to "critical" in its rating scale.

A Microsoft representative said the company is aware of the exploit code but is unaware of active attacks that have utilized it. Microsoft is monitoring the situation and is urging customers to apply its patch, the representative said. The company also directed people to report any attacks to Microsoft and the FBI.

The vulnerability has been found in several versions of Outlook Express, including releases 5.5 and 6.0 for Windows 2000, XP and Server 2003 machines, according to Microsoft. People don't have to launch the Outlook Express program, however, in order to fall victim to an attack.

Source [2].

Microsoft

Links:

[1] http://www.tuxmachines.org/taxonomy/term/62
[2] http://news.com.com/Hackers+probe+Outlook+Express+flaw/2100-7349_3-5761537.html?tag=nefd.top