

## Vista: Faces security storm again!

After last week's ShoutHack flaw, Microsoft's recently-released operating system Windows Vista is once again in the eye of a security storm. It is possible to elevate the system privileges by exploiting a flaw in Vista, according to vulnerability researchers.

In an interview at the ongoing global security conference RSA 2007, Marc Maiffret, CTO and chief hacking officer of California-based eEye Digital Security Inc, said that there's a way to use a non-Microsoft vulnerability to remotely compromise Vista, as well as a way to elevate the system privileges using a Vista-specific flaw, according to technology websites.

This is a vulnerability specific to Vista that doesn't exist in XP. Interestingly, Microsoft has made a lot of security improvements in Vista, but it is becoming obvious that a few loopholes will always escape attention. Maiffret plans to demonstrate his findings later this week at the IT-Defense 2007 conference in Germany.

Incidentally, this is not the first time that a security expert has warned of a flaw in Vista at the RSA conference. Vulnerability researchers at Boston-based Core Security Technologies have also claimed that a well-known vulnerability existing in Computer Associates' BrightStor backup software can be exploited when the programme is running on Vista.

Company officials announced the flaw immediately after the Microsoft chairman Bill Gates delivered his keynote address. Penetration testing software-maker Core has contended that a previously disclosed vulnerability in CA's BrightStor ARCserve Backup software, dubbed CVE-2007-0169, can be exploited to compromise systems running Vista.

The vulnerability suggests that in a rush to roll out Vista-compatible software, third parties might ignore some of the security features in the new OS.

Microsoft has said Vista is its most secure OS to date, and features like Address Space Layout Randomization (ASLR) are meant to insulate Vista from malware attacks. However, unless application vendors such as CA integrate with those features, the tools can be easily defeated, as pointed out by the BrightStor exploit.

Last week, the technology media was abuzz with what was supposedly the first Vista flaw. It is said that the flaw allows remote attackers to take advantage of Vista's speech recognition feature.

The potential security hole was discovered after an online discussion prompted a blogger to try out a speech-based hack. The blogger reported on technology website ZDNet that he was able to access the Vista Start menu and, run programmes using voice commands played over the system's speakers.

According to reports, several Vista users tested the exploit and were able to delete files and empty the Trash Can so that the documents were not retrievable. In one scenario outlined by users, an MP3 file of voice instructions was used to tell the PC to delete documents.

***EconomicTimes.com 07.02.07***



cirosec GmbH  
Edisonstraße 21  
74076 Heilbronn  
Tel: 07131 / 59455-0  
Fax: 07131 / 59455-99  
info@cirosec.de  
[www.cirosec.de](http://www.cirosec.de)