

13 July 2006

By: Marius Oiaga, Technology News Editor



Adobe Patched 2 Reader Vulnerabilities

One of them was ranked as critical

The Adobe Acrobat and Reader application from Adobe has managed to spread its vulnerabilities both to Windows and to Mac operating systems. On July 12, Adobe Systems joined Microsoft on a patching campaign, although the problems it faced were not as numerous as Microsoft's. Security companies have warned that if left unpatched, the vulnerabilities could have allowed for remote code execution, a condition sufficient enough that one of the two Adobe flaws was ranked as critical. The two flaws refer to Adobe Acrobat and Reader insecure default permissions and a buffer overflow in distilling to PDF. The first one affects Mac OS X. "A vulnerability has been reported in Adobe Acrobat and Adobe Reader, which can be exploited by malicious, local users to bypass certain security restrictions or gain escalated privileges. The vulnerability is caused due to insecure default file permissions being set on the installed files and folders. This allows any non-privileged users on the system to remove the files or replace them with malicious binaries. The vulnerability has been reported for Adobe Acrobat 6.0.4 and Adobe Reader 6.0.4 for Mac OS. Prior versions may be also affected," disclosed security company Secunia. The second vulnerability allows for arbitrary code execution and may cause a buffer overflow condition on the system. This flaw is shared by both Windows and Mac OS and could be exploited on the distillation of a document into PDF file format. "This condition presents a risk for shared, multiuser systems," Adobe said. "On such systems, a hostile unprivileged user could take advantage of this condition to replace these program files with malicious or harmful code that could read, write or destroy sensitive data if subsequently run by a privileged user."