IN A harbinger of security threats to come, hackers have exploited a newly announced flaw in Microsoft programs and begun circulating malicious code hidden in images that use the popular JPEG format. Software tools to create the malicious images began appearing last month, and this week security experts saw images employing them posted on adult-oriented Usenet newsgroups.

To get the malicious code, a visitor must download the image and view it using Microsoft's Windows Explorer software, said Oliver Friedrichs, senior manager with Symantec Security Response.

The computer then contacts a server to obtain code that would let an attacker take over the machine remotely.

Mr Friedrichs said the current exploit is fairly limited but that he expects future attempts to create malicious images that would work on the more popular Outlook and Internet Explorer programs, also made by Microsoft.

The internet Storm Centre at the SANS Institute said an image it found, disclosed on the BugTraq security mailing list, only caused computers to crash in tests, but "we suspect that a working exploit is very close to widespread availability".

Computers with updated versions of anti-virus software should be protected, according to the SANS centre. Microsoft also has a software patch to fix the flaw and said users who have the Service Pack 2 security update for Windows XP are not affected.


People who have earlier versions of Windows or Office may also be affected if they are running some specialised applications, such as Digital Image Pro and Visio 2002. The flaw is in a technology that is used to render JPEG images.

*The Associated Press*

This report appears on australianIT.com.au.