

## Vulnerability in Graphics Rendering Engine Could Allow Remote Code Execution

### Introduction

WMF images file is being used by attackers to run malicious code. This malicious code is being executed the moment the image is being viewed. User does not necessarily need to click on the image file in order to trigger the exploit; it will be executed by just viewing the image, which can be done by viewing directory with the explorer showing icon size image or using desktop indexing software or just visiting a web site that has an image file containing the exploit.

### What is WMF format?

Windows Metafile is a 16-bit metafile format that can contain both vector information and bitmap information. WMF files containing a sequence of GDI (graphical-device-interface) function calls. The image is created by executing these functions.

The security problem is with some GDI functions, the exploit is using some of the functions (e.g. SETABORTPROC GDI Escape function) to execute arbitrary code when the image is viewed.

### Affected Versions

- Windows 2000
- Windows XP (SP1 & SP2)
- Windows 2003
- Win9x, WinME and Win2k are vulnerable but require user intervention

### Attack Vectors

- Internet Explorer is a common attack vector for this vulnerability (in its default settings).
- Windows Picture and Fax Viewer or any other application that can open a file with the associated program for that file type (e.g. ShellExecute)

### Protection

Vital Security™ Web Appliance customers are protected against WMF vulnerability. Microsoft has release a special fix for that critical vulnerability (MS06-001)

### Finjan's Solution

Utilizing its patented behavior-based security technologies, Finjan delivers the ONLY proactive content security solution capable of protecting companies from new, unknown attacks arriving via the web the first time they strike. Using this patented technology, Finjan's Vital Security™ solutions provide superior protection against complex web-borne attacks, such as Spyware, Phishing/Pharming, Trojans and malicious code.

### References

- <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560>
- <http://www.microsoft.com/technet/security/bulletin/ms06-001.msp>
- <http://www.kb.cert.org/vuls/id/181038>
- <http://secunia.com/advisories/18255/>
- [http://vil.mcafeesecurity.com/vil/content/v\\_137760.htm](http://vil.mcafeesecurity.com/vil/content/v_137760.htm)
- <http://www.securityfocus.com/bid/16074/info>