

[News](#)[Articles](#)[Press](#)[Releases](#)[Downloads](#)[Privacy](#)[Policy](#)[RSS Feeds](#)[Channels](#)[IT Security](#)[Insight](#)[Storage](#)[Reviews](#)[Editorials](#)[Wireless](#)[About ITO](#)[Advertise](#)[Whitepapers](#) [RSS Feed](#)

Malicious code targets Unpatched flaw in Internet Explorer

Friday, 22 September 2006 10:00 EST

A critical vulnerability is identified in Internet Explorer versions 5+ and above. Security experts at MicroWorld Technologies say a malicious code named 'Exploit.HTML.VML' is being actively exploited by Pornographic and other shady websites to install Spyware and Trojans into user computers without their knowledge.

The vulnerability is found in the implementation of VML -Vector Markup Language- derived from XML and used in delivering vector graphics with geometrical shapes and mathematical equations, in Internet Explorer. File formats such as SWF(Flash), PDF(Adobe Acrobat), AI (Adobe Illustrator), EMF (Microsoft Enhanced Metafile) are examples of vector graphics.

'Exploit.HTML.VML' pushes other malware into computers by inducing a Stack Buffer Overflow, when a smartly crafted page with VML containing a long "fill" method inside a "rect" tag, is displayed in IE. In a typical scenario, Internet Explorer is seen crashing soon after the exploit is delivered.

Microsoft has confirmed that the vulnerability allows the malware author to execute arbitrary code on the attacked system while acknowledging that a successful intruder can gain local user rights on victim's computer. The corporation is working on a patch for the flaw and if the situation warrants, would go for an earlier release of it, before its monthly patching cycle scheduled on October 10.

"This is a Drive-by Download Attack using a Zero-day vulnerability, making it a definite case of clear and present danger," says CEO of MicroWorld Technologies, Govind Rammurthy. "Just by visiting shady websites, community portals or photo exchange sites where user posted content is hosted without much supervision, you could well be inviting sly malware right into your PC."

Acunetix Web Security Scanner

Check your website security with a FREE **website security audit** by **Acunetix**. Audit your web applications for **SQL injection**, **cross site scripting** & more with **Acunetix Web Vulnerability Scanner**

GFI LANguard Security Scanner

Is your network open to attack? Find out with the #1 sold network security scanner: GFI LANguard Network Security Scanner! **Download your FREE trial version today.**



Downloads

- » [BeEF - Browser Exploitation Framework 0.2.1](#)
- » [TrackMeNot - Firefox extension to protect against data-profiling 0.3.0a](#)
- » [fwknop - Single Packet Authorization 0.9.7](#)
- » [Wapiti - Web application vulnerability scanner 1.1.3](#)
- » [SSH Tunnel Manager 1.2](#)

Press Releases

- » [Internet Security Systems Seen As 'Trusted Security Advisor' By Its EMEA Channel Partners](#)
- » [Special Operations Software Announces Another Record Year of Revenue Growth](#)
- » [Aventail's SSL VPN ST2 Replacement of Leading IPsec VPNs Demonstrates Growing Market Trend](#)
- » [SAND Technology Demonstrates Interoperability with Network Appliance Enterprise Storage and Compliance Solutions](#)
- » [CryptoCard Partners with Value-Added Reseller, 2Build4 BV, to Provide Dutch Businesses With](#)

[Truly User-Friendly and Cost Effective Two-Factor Authentication](#)

Reviews

- » [CA Anti-Spam 2007](#)
- » [System Safety Monitor 2.1](#)
- » [CA Personal Firewall 2007](#)
- » [Safend Auditor - Review](#)
- » [Web Application Code Auditing with SWAAT](#)

Copyright © IT-Observer.com 2000 - 2006