



SA Computer MAGAZINE



Latest News

Flaw in Internet Explorer Rings Security Alarm

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."

Mail Clients like Outlook Express that preview emails, using IE rendering mechanism, is also at equal risk, says Govind Rammurthy. Potential large scale attacks via email using VML embedded HTML, can be launched to invade user computers, where all you need is to view the mail, to be ambushed.

About Us

Latest Issue



**OCTOBER
2006**

**LAMBORGHINI
VS. FERRARI:**
Which hot-road
notebook
takes the
chequered
flag? Includes
Cover CD!

On shelf 28 September
[[Subscribe](#)]

Contact Details

[tel] +27 11 704 2679
[fax] +27 11 704 4120

[Subscriptions](#)

[Advertising](#)

[Webmaster](#)



MicroWorld Security analysts suggest following actions to safeguard computers till the patch is out:

- Keep eScan and MailScan updated regularly
- Stay away from pornographic, murky and community websites.
- Use a powerful Spam Stopper that uses a combination of Anti Spam Techniques.
- Disable the Preview option in Outlook Express.
- Modify the Access Control List on 'Vgx.dll' to add more restrictions.
- Disable Java script and Active-X controls in IE, as some variants of the exploit are using these routes.

Press Release / *Posted on 22 Sep 2006*

Content Management Powered by [CuteNews](#)

[archives](#) / 

All content (c) SA Computer Magazine, All Rights Reserved.