

<i>IT Management Begins With Security</i>		WebProWorld Security Forum		RSS	Subscribe to our RSS feed . Stay current with our latest!
	Breaking Security Related News Your Source for investigative security related reporting and breaking news				
HOME	IT ARTICLES	NEWS	NEWSLETTER ARCHIVES	ABOUT US	ADVERTISE
			SUBMIT AN ARTICLE		

SecurityProNews > News > Security News > **Microsoft Releases Early Patch For The VML Flaw**

Search:

[news_security_news]

Microsoft Releases Early Patch For The VML Flaw

Btv Raj
Contributing Writer
2006-09-27

[SecurityProNews: News RSS Feed](#)

[Security News RSS Feed](#)

[PRINT VERSION](#) [EMAIL](#) [BOOKMARK](#)

Microsoft Corporation broke its patch Tuesday cycle falling on second Tuesday of every month, to release a fix for the critical and widely exploited VML vulnerability in Internet Explorer.

Security Experts at the AntiVirus and Content Security firm, MicroWorld Technologies, urge computer users to go for an immediate update of the Explorer patch.

The patch released yesterday can be found at <http://www.microsoft.com/technet/security/bulletin/ms06-055.mspx>. It plugs the remote code execution vulnerability in the Vector Markup Language (VML), when a smartly crafted webpage with VML containing a long "fill" inside a "rect" tag is displayed in IE.

Microsoft was under pressure as the number of websites hosting malicious exploits for the vulnerability grew multifold while scamsters sent out spoof ecards, leading users to many sites that dropped Keyloggers into user computers via the flaw. 0

"The potential risk level of a vulnerability depends on multiple factors than the mere gravity of the software flaw," says Govind Rammurthy CEO, MicroWorld Technologies. "Different attack vectors, availability of the exploit code, the amount of user interaction required for a successful penetration and the level of organizing and coordination displayed in the attack, all contribute towards how serious the threat can become within a short span of time. In that sense, this VML vulnerability had all the right ingredients to make you dash for cover."

SecurityProNews

NetworkingFiles

ITManagementNews

FENTRY Help Center

[Top Stories](#)

VIRUS WARNINGS

Newsletter Signup

Subscribe to SecurityProNews FREE!

[[more newsletters](#)]

Featured On:

AS FEATURED ON
NEWS NOW

article resources

Search Articles:

[[advanced search](#)]

WebProWorld.com

- **Get in-touch** with industry experts and leaders
- **Post** your site for review by expert and peers
- **Ask** Security, IT, Development and Design questions

Free Membership: [Join Now!](#)

Visit [WebProWorld.com](#)

An imminent possibility of changing vectors and targets loomed in the form of mass mailing attacks aiming at Outlook and Outlook Express, both using IE's rendering mechanisms to preview emails. It meant the attacker can compromise and takeover a remote computer with little or no action from the victim's side.

In the mean time, a security group named Zero Day Emergency Response Team (ZERT) offered an unofficial patch for the vulnerability, presenting users with the tough choice between perils of a critical browser vulnerability and a possible software clash arising from a third party component. The plot got thicker with the second unofficial patch coming from a vulnerability management firm, Patchlink.

The confusion now settles down with the release of the Microsoft patch which blocks the hole in the risky VML component, but not before raising serious questions about the effectiveness, safety and legitimacy of third party patches for vulnerabilities in software applications.

MicroWorld Solutions eScan and MailScan were soon updated with protection against the exploit code in the wild named Exploit.HTML.VML, while also providing workarounds for mitigating the threat. The security firm protects its users with its fastest updating Threat Detection and Prevention System, Advanced Behavioral Analysis and the unique MWL technology. eScan and MailScan also employ a Multi-pronged Spam Blocking system to make sure that emails carrying malware do not make it to user mailboxes. To prevent network Intrusions, MicroWorld offers eConceal Firewall and for best of breed spam protection, X-Spam.

"Be it large Enterprises or home users, two major channels of malware proliferation are Web Access and emails, amply displayed in the case of this exploit. One needs to be extra careful in guarding these prime conduits, as Virus writers and hackers find and force errors via these routes to advance their cause. We at MicroWorld combine some of the future defining technologies to combat and prevent digital threats in a continuous and consistent fashion, to ensure that we leave nothing to chance," says Sunil Kripalani, Vice President, Global Sales and Marketing, MicroWorld Technologies.

MicroWorld

MicroWorld Technologies (www.mwti.net) is the developer of the world's most advanced AntiVirus and Content Security software eScan for desktops and servers. Its gateway-level email security software, MailScan, is a comprehensive mail scanner for your SMTP/POP3 Mail Servers. MicroWorld Winsock Layer (MWL) is the revolutionary technology underlying these products, powering them to several certifications and awards by some of the most prestigious testing bodies, notable among them being Virus Bulletin, Checkmark, TUCOWS, Red Hat Ready and Novell Ready. On the Network Security side, MicroWorld offers a powerful, futuristic network firewall branded as eConceal.

About the Author:

To learn more, kindly visit <http://www.mwti.net>.

Btv Raj is the Content Writer and Creative Visualizer, MicroWorld Technologies.

[More news_security_news Articles](#)

SecurityProNews: News
RSS Feed

[Security News RSS Feed](#)



iEntry Featured Services: [Jayde Member Services](#) | [Forums](#) | [Freeware](#) | [Advertise with Us](#)

[Contact Us](#) | [Advertise](#) | [Newsletter Archive](#) | [Sitemap](#) | [Submit an Article](#) | [News Feeds](#)

SecurityProNews is an [iEntry, Inc.](#)® publication - All Rights Reserved | [Privacy Policy](#) and [Legal](#)

Join the WebProWorld Forums: [Click Here](#)