

IT Backbones - Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links



Give your mouse a heart!

search 

Dedicated To IT Security Issues, Featuring News, Press Releases, IT Directory & Links

- [Home](#)
- [About](#)
- [Contact](#)
- [Submit PR](#)
- [Search News](#)
- [What We Can Offer You](#)
- [IT Events](#)
- [Time & Money](#)

New Vulnerability Exposed in Microsoft PowerPoint

Published 4th October 2006

A new vulnerability has been identified in Microsoft PowerPoint. In a fortnight plagued with vulnerabilities and patches like never before, this new flaw allows Remote Code Execution on targeted computers, inform Security Analysts at MicroWorld Technologies.

Using the vulnerability, a remote attacker can execute arbitrary code on a targeted machine, by exploiting the memory corruption occurring when a smartly created PowerPoint file with the exploit code, is opened in Office 2003, Office 2000 and Office XP and also in PowerPoint 2004 for Mac OS X and PowerPoint v. X for Mac OS X.

Two exploits targeting the flaw, already in the wild, are detected as MSPPoint.Agent.k and MSPPoint.Agent. These malwares drop a backdoor named Backdoor.Ginwui, the same Trojan used in the May-2006 attack via MS word files.

Once inside the computer, the backdoor can log off current user, harvest system information, stop and start processes, download files from the net and execute them, capture network user information, search disks for files and do more as desired by the far away hacker.

Microsoft has acknowledged the vulnerability and says as a best practice, users should always exercise extreme caution when opening unsolicited attachments from both known and unknown sources. As a workaround for the security hole, the

Redmond Corporation suggests users view PowerPoint files received via emails or Internet using PowerPoint Viewer 2003, as it does not have the said vulnerability.

“The Vulnerability and patch story has long become a cat and mouse game,” says Govind Rammurthy, CEO, MicroWorld Technologies. “Though the regular exposure of Windows vulnerabilities has become commonplace for some years now, the year 2006 has hit the roof when it comes to MS office vulnerabilities. You can see many flaws being unearthed in MS Office 2000, 2003, with some unprecedented enthusiasm displayed by vulnerability researchers and malicious hackers.”

Govind Rammurthy cautioned that users will need to be on their guards while dealing with files from unknown senders, as there are multiple vulnerabilities reported in MS Office applications like Word and PowerPoint recently. Patching all software, keeping the Antivirus updated and protecting computers with Firewalls are key steps in safeguarding Information systems.

MicroWorld Technologies, the world’s most advanced AntiVirus and Content Security Solution provider, protects their users from a wide range of exploits and Trojan Droppers that target vulnerabilities in Operating systems and Applications. While eScan and MailScan from MicroWorld technologies work on a combination of futuristic technologies to ward off online threats, its eConceal Firewall presents a Comprehensive Intrusion Detection and Prevention System.

Company Profiles powered by ITReseller.com

- MicroWorld Technologies Inc - [View profile](#)

[Links](#) | [About Us](#) | [Privacy Policy](#) | [Contact Us](#) | © 2004-2006 IT Backbones Limited

Site developed and hosted by [Design Solution](#) Ltd.