eEye Digital Security®

Know your vulnerabilities. Know you're protected.

Vulnerability Expert Forum

April 11, 2012

Agenda

- About eEye
- Microsoft's April Security Bulletins
- Security Landscape: Other InfoSec News
- Secure and Comply with eEye
- Q&A

eEye Digital Security®

eEye at a Glance

Industry Pioneers

- Leaders in IT security since 1998
- Developed one of the first vulnerability scanners
- Growing and profitable

Thought Leaders

- World-renowned security research team
- Trusted advisors to organizations across industries and sizes

Security Experts

- Seasoned security professionals
- Thousands of customers
- Some of the largest VM installations in the world

Award-Winning Solutions

- Recognized product leadership
- Securing companies of all sizes
- Unparalleled services and support

eEye Digital Security®

Why eEye

- **Making the Complex Simple**
- Unified
- Efficient
- Effective

The Industry Experts Say…

"Retina provides a solid feature set with easy-to-use scanning controls. It's an excellent vulnerability scanner at a good price. This one gets our Best Buy."

SC MAGAZINE

"eEye Digital Security raises the standard in enterprise endpoint protection with a management console that could almost be called next generation."

eWEEK BUILDING THE E-BUSINESS ENTERPRISE

"eEye's security research team continues to provide good Windows vulnerability coverage and mitigation advice for zero-day vulnerabilities."

Gartner

"Retina has many desirable features…and an extremely flexible reporting portal. The product is also attractively priced."

FORRESTER

eEye Digital Security®

eEye Research Services

eEye Preview

- Advanced Vulnerability Information
- Full Zero-Day Analysis and Mitigation
- Custom Malware Analysis
- eEye Research Tool Access
- Includes Managed Perimeter Scanning

eEye AMP

- Any Means Possible Penetration Testing
- Gain true insight into network insecurities
- “Capture-The-Flag” Scenarios

eEye Custom Research

- Exploit Development
- Malware Analysis

Forensics Support

- Compliance Review

eEye Digital Security®

Microsoft April Security Bulletins

- 6 Total Bulletins; 11 Issues Fixed
  - Cumulative Security Update for Internet Explorer (2675157)
  - Vulnerability in Windows Could Allow Remote Code Execution (2653956)
  - Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)
  - Vulnerabilities in Forefront Unified Access Gateway (UAG) Could Allow Information Disclosure (2663860)
  - Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258)
  - Vulnerability in Microsoft Office Could Allow Remote Code Execution (2639185)

eEye Digital Security®

Microsoft Security Bulletin: MS12-023

- 5 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0168 - Print Feature Remote Code Execution Vulnerability
  - CVE-2012-0169 - JScript9 Remote Code Execution Vulnerability
  - CVE-2012-0170 - OnReadyStateChange Remote Code Execution Vulnerability
  - CVE-2012-0171 - SelectAll Remote Code Execution Vulnerability
  - CVE-2012-0172 - VML Style Remote Code Execution Vulnerability
- Severity: Critical
- Whole Lotta RCE
  - Affects all versions of IE
  - Maliciously crafted HTML attack vector
- Mitigations
  - Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting
  - Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting

eEye Digital Security®

Microsoft Security Bulletin: MS12-024

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0151 - WinVerifyTrust Signature Validation Vulnerability
- Severity: Critical
- WinVerifyDistrust
  - Attackers can modify existing signed executables
  - Make Notepad.exe malicious :-D
  - Oops.
- Mitigations
  - Nada.

eEye Digital Security®

Microsoft Security Bulletin: MS12-025

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0163 - .NET Framework Parameter Validation Vulnerability
- Severity: Critical
- .RCE
  - Can bypass Code Access Security (CAS)
  - Attacker can host malicious XBAP and convince users to visit
  - Perfect for Exploit Packs
- Mitigations
  - Disable XAML browser applications in Internet Explorer

eEye Digital Security®

Microsoft Security Bulletin: MS12-026

- 2 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0146 - UAG Blind HTTP Redirect Vulnerability
  - CVE-2012-0147 - Unfiltered Access to UAG Default Website Vulnerability
- Severity: Important
- Forefront Unified Information Disclosure Gateway
  - Remote information disclosure via specially crafted query
  - Changes binding settings to restrict access to internal resources
- Mitigations
  - None at this time

eEye Digital Security®

Microsoft Security Bulletin: MS12-027

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0158 - MSCOMCTL.OCX RCE Vulnerability
- Severity: Critical
- ActiveX RCE? Who would have guessed.
  - Office/WordPad documents, malicious websites
  - Reports of limited attacks in-the-wild
- Mitigations
  - Do not open Microsoft Office and WordPad documents from untrusted sources
  - Prevent the vulnerable ActiveX controls from being run in Internet Explorer

eEye Digital Security®

Microsoft Security Bulletin: MS12-028

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0177 - Office WPS Converter Heap Overflow Vulnerability
- Severity: Important
- I miss DLL hijacking ☹
  - Heap overflow
  - Works? Lol.
  - Caused by a bad header field value, used in a memcopy
- Mitigations
  - Do not open Works files that you receive from untrusted sources or that you receive unexpectedly from trusted sources

eEye Digital Security®

April Giveaway: Win a Kindle Fire!

Recently the eEye Research Team released the whitepaper "In Configuration We [Still] Trust" along with a free config check tool. The goal of that research was to draw awareness to the fact that a lot of security improvement can be made simply by how you architect your network and configure your operating systems and applications.

How to Win: Answer the Question Below

"What are some real-world ways IT can improve security?"

Post Your Answer (and download the free tool) at: eeye.co/aprilvefgiveaway

Deadline: Friday, April 13, 3pm PT

**Giveaway open to US residents only, because Canada is too far.*

eEye Digital Security®

Security Landscape - *More than a Microsoft World*

- CTO/CSO/CxO News
  - Medicaid hacked: over 181,000 records and 25,000 SSNs stolen
  - Major Credit Card Processor
  - Shopping for 0day
  - More Chinese Industrial Espionage
- IT Admin News
  - Mozilla Adds Older Java Versions to Firefox Blocklist
  - Flashback Mac Malware Detection Tool
  - Flash Auto-Updater
- Researcher News
  - WebServices Auditing
  - First Android Bootkit Found
  - Apple Battles Flashback Trojan With Second Mac Update
  - European Union Moves to Criminalize 'Hacking Tools'

eEye Digital Security®

Retina CS Community

RETINA Community

RETINA Network Community
Free Vulnerability Scanner (up to 128 IPs)

RETINA CS Community
Free Vulnerability Management (up to 128 IPs)

- *New* Retina CS Community
  - Free version of Retina CS for up to 128 IPs
    - Reduce security risks with the most cost-effective vulnerability management product available
    - Streamline remediation with automated patching for both Microsoft and third-party applications
    - Increase visibility and automate vulnerability scanning for BlackBerry mobile devices and virtualized apps
- Download Now: http://community.eeye.com/

eEye Digital Security®

Connect with eEye

- http://blog.eeye.com
- http://www.facebook.com/eEyeDigitalSecurity
- http://www.twitter.com/eEye
- http://www.YouTube.com/eEyeDigitalSecurity

eEye Digital Security®

eEye Security Risk Management

Risk Management & Visibility

- End-to-end vulnerability and compliance management
- Centralized management, reporting, and controls
- Discover, prioritize, and remediate from one console
- Advanced trending and interactive risk analytics

Risk Discovery

- Local, Remote, Physical, and Virtual Assets
- Private Cloud and Mobile Devices
- Flexible, Dynamic Asset Scoping
- Unified VA and Config Scanning
- Zero-Day Vulnerability Identification

Risk Prioritization

- Flexible Risk Scoring
- Broad Exploit Intelligence
- Integrated Attack and Malware Info
- Exception Tracking and Reporting
- Risk-based Reporting

Risk Remediation

- Built-in Patch Management
- Integration with Key Patch Vendors
- Integrated Protection for Zero-Days and Advanced Persistent Threats
- Integrated Malware and Attack Protection and Reporting

Security Research

eEye Security Risk Management = Reduced Risk & Lower TCO

eEye Digital Security®

Start Today

→Visit eEye

http://www.eEye.com

- About Us, Solutions, Awards, Resources, Downloads

→Visit the eEye Security Resource Center

http://www.eEye.com/Resources

- Patch Tuesday Information, Demos, Guides, Whitepapers, Videos, Webinars, Events

→Contact Us

1.866.339.3732 or research@eEye.com

eEye Digital Security®