eEye Digital Security®

Know your vulnerabilities. Know you're protected.

Vulnerability Expert Forum

May 9, 2012

Agenda

- About eEye
- Microsoft's May Security Bulletins
- Security Landscape: 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 May Security Bulletins

- 7 Total Bulletins; 23 Issues Fixed
  - Vulnerability in Microsoft Word Could Allow Remote Code Execution (2680352)
  - Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2663830)
  - Vulnerability in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (2597981)
  - Vulnerability in TCP/IP Could Allow Elevation of Privilege (2688338)
  - Vulnerability in Windows Partition Manager Could Allow Elevation of Privilege (2690533)
  - Combined Security Update for Microsoft Office, Windows, .NET Framework, and Silverlight (2681578)
  - Vulnerabilities in .NET Framework Could Allow Remote Code Execution (2693777)

eEye Digital Security®

Microsoft Security Bulletin: MS12-029

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0183 - RTF Mismatch Vulnerability
- Severity: Critical
- YaarrrrRTF!
  - Privately reported vulnerability
  - RTF parser in Word parses more than just characters :-O
  - Always a good idea to not run as admin
- Mitigations
  - Read emails in plain text
  - Use Microsoft Office File Block policy to block the opening of RTF documents from unknown or untrusted sources and locations

eEye Digital Security®

Microsoft Security Bulletin: MS12-030

- 6 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0141 - Excel File Format Memory Corruption Vulnerability
  - CVE-2012-0142 - Excel File Format Memory Corruption in OBJECTLINK Record Vulnerability
  - CVE-2012-0143 - Excel Memory Corruption Using Various Modified Bytes Vulnerability
  - CVE-2012-0184 - Excel SXLI Record Memory Corruption Vulnerability
  - CVE-2012-0185 - Excel MergeCells Record Heap Overflow Vulnerability
  - CVE-2012-1847 - Excel Series Record Parsing Type Mismatch
- Severity: Important
- Excel Spreads Some Sheet
  - Multiple memory corruptions due to improperly validated data
- Mitigations
  - Use Microsoft Office File Block policy to block the opening of Office 2003 and earlier documents from unknown or untrusted sources and locations
  - Use MOICE, set Office File Validations to disable files that fail validation

eEye Digital Security®

Microsoft Security Bulletin: MS12-031

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0018 - VSD File Format Memory Corruption Vulnerability
- Severity: Important
- RCE in VSD
  - Visio improperly validates attributes in VSD files
  - Could allow for arbitrary remote code execution
- Mitigations
  - Set Internet and Local intranet security zone settings to "High" to block ActiveX Controls and Active Scripting in these zones
  - Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone
  - Do not open Office files that you receive from untrusted sources or that you receive unexpectedly from trusted sources

eEye Digital Security®

Microsoft Security Bulletin: MS12-032

- 2 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0174 - Windows Firewall Bypass Vulnerability
  - CVE-2012-0179 - TCP/IP Double Free Vulnerability
- Severity: Important
- TCP/IP EoP
  - One publicly disclosed, one privately disclosed
  - Allows for Firewall bypass (outbound broadcast packets)
  - TCP/IP IPv6 improperly handles binding, allowing for EoP
- Mitigations
  - No practical mitigations

eEye Digital Security®

Microsoft Security Bulletin: MS12-033

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0178 - Plug and Play (PnP) Configuration Manager Vulnerability
- Severity: Important
- Plug and Elevation of Privilege
  - Successful exploitation could allow for arbitrary code execution in kernel mode
  - Issue with Partition Manager handling device relation requests
- Mitigations
  - No practical mitigations available

eEye Digital Security®

Microsoft Security Bulletin: MS12-034

- 10 Vulnerabilities Fixed in Bulletin
  - CVE-2011-3402 – TrueType Font Parsing Vulnerability
  - CVE-2012-0159 – TrueType Font Parsing Vulnerability
  - CVE-2012-0162 – .NET Framework Buffer Allocation Vulnerability
  - CVE-2012-0164 – .NET Framework Index Comparison Vulnerability
  - CVE-2012-0165 – GDI+ Record Type Vulnerability
  - CVE-2012-0167 – GDI+ Heap Overflow Vulnerability
  - CVE-2012-0176 – Silverlight Double-Free Vulnerability
  - CVE-2012-0180 – Windows and Messages Vulnerability
  - CVE-2012-0181 – Keyboard Layout File Vulnerability
  - CVE-2012-1848 – Scrollbar Calculation Vulnerability

eEye Digital Security®

Microsoft Security Bulletin: MS12-034 Continued

- Severity: Critical
- I don't think this bulletin covered enough products…
  - Three vulnerabilities were publicly disclosed
  - Multiple attack vectors
  - Embedded TTF in websites
  - Issues with GDI+ validating EMF record types and EMF images
- Mitigations
  - Deny access to T2EMBED.DLL
  - Disable XAML browser applications in Internet Explorer
  - Disable metafile processing

eEye Digital Security®

Microsoft Security Bulletin: MS12-035

- 2 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0160 - .NET Framework Serialization Vulnerability
  - CVE-2012-0161 - .NET Framework Serialization Vulnerability
- Severity: Critical
- Super Serial You Guys…
  - Remotely exploitable
  - Improper serialization of untrusted input via untrusted and partially trusted assemblies
- Mitigations
  - Disable partially trusted Microsoft .NET applications
  - Disable XAML browser applications in Internet Explorer

eEye Digital Security®

May Giveaway: Win a Kindle Fire!

Recently eEye announced the release of Retina CS 3.1. Version 3.1 expands our market leadership in innovation for helping IT secure the technologies being widely deployed today.

How to Win: Answer the Question Below

"How are you currently managing mobile and/or cloud security intelligence?"

Post Your Answer at: eeye.co/mayvefgiveaway

Deadline: Friday, May 13, 3pm PT

**Giveaway open to US residents only*

eEye Digital Security®

Security Landscape - *More than a Microsoft World*

- CTO/CSO/CxO News
  - Google Drive
  - A/V Fails to Detect APT, Simple Evasion Techniques
  - Apple Leads Number of Vulns for Q1
- IT Admin News
  - Java 6 Tweaked in OS X
  - Oracle to Deliver OS X JVM Directly
  - Windows 8 Enterprise Exclusive Features
- Researcher News
  - Google Ups Bounty For Bugs To $20,000
  - Amazon Cloud now 1% of all Internet Traffic
  - Researchers Find that Some Cloud Services do not Zero out Virtual Drives
  - New Exploit Pack - Redkit

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®