eEye Digital Security®

Know your vulnerabilities. Know you're protected.

Vulnerability Expert Forum

March 15, 2012

Agenda

- About eEye
- Microsoft's March 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 March Security Bulletins

- 6 Total Bulletins; 7 Issues Fixed
  - Vulnerability in DNS Server Could Allow Denial of Service (2647170)
  - Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)
  - Vulnerability in DirectWrite Could Allow Denial of Service (2665364)
  - Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)
  - Vulnerability in Visual Studio Could Allow Elevation of Privilege (2651019)
  - Vulnerability in Expression Design Could Allow Remote Code Execution (2651018)

eEye Digital Security®

Microsoft Security Bulletin: MS12-017

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0006 – DNS Denial of Service Vulnerability
- Severity: Important
- DNSpwned
  - Denial of Service caused by heap overflow
  - Triggered by millions of unique/wildcard DNS domain queries
  - Can be triggered over a long period time or in a flood of queries
- Mitigations
  - Periodically clear the DNS Cache

eEye Digital Security®

Microsoft Security Bulletin: MS12-018

- 1 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0157 – PostMessage Function Vulnerability
- Severity: Important
- Kernel-Pwned
  - Access violation in ring0 context
  - Most likely used in a two-part attack
- Mitigations
  - No reasonable mitigation currently exists.

eEye Digital Security®

Microsoft Security Bulletin: MS12-019

- 1 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0156 – DirectWrite Application Denial of Service Vulnerability
- Severity: Moderate
- DirectPwned
  - Unicode parsing issue
  - Anything using DirectWrite is susceptible to this vulnerability
- Mitigations
  - No reasonable mitigation currently exists.

eEye Digital Security®

Microsoft Security Bulletin: MS12-020

- 2 Vulnerabilities Fixed in Bulletin
  - CVE-2012-0002 – Remote Desktop Protocol Vulnerability
  - CVE-2012-0152 – Terminal Server Denial of Service Vulnerability
- Severity: Critical
- RDPwned
  - Wormable issue with the RDP protocol
  - Default configuration not susceptible to attack
  - However, RDP widely enabled ;-)
- Mitigations
  - Disable Terminal Services, Remote Desktop, Remote Assistance, and Windows Small Business Server 2003 Remote Web Workplace
  - Block TCP port 3389 at the enterprise perimeter firewall
  - Enable Network Level Authentication

eEye Digital Security®

Microsoft Security Bulletin: MS12-021

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0008 – Visual Studio Add-In Vulnerability
- Severity: Important
- Visual Studio Add-PWNED
  - Lower privilege attacker positions malicious add-in
  - Add-in references malicious DLL
  - Convince target to run Visual Studio as Admin
- Mitigations
  - Avoid running Visual Studio with elevated privileges

eEye Digital Security®

Microsoft Security Bulletin: MS12-022

- 1 Vulnerability Fixed in Bulletin
  - CVE-2012-0016 – Expression Design Insecure Library Loading Vulnerability
- Severity: Important
- Not Everything Stays in Vegas
  - The end is nigh
- Mitigations
  - Disable loading of libraries from WebDAV and remote network shares
  - Disable the WebClient service
  - Block TCP ports 139 and 445 at the firewall

eEye Digital Security®

March Giveaway: Win a Kindle Fire!

A recent stat provided by CNN Money stated that "61% of Adobe Reader plug-ins are outdated on work computers."

How to Win: Answer the Questions Below

"Does the stat above surprise you? Why or why not? How are you managing non-Microsoft patching today?"

Post Your Answer at: eeye.co/marvefgiveaway

Deadline: Friday, March 16, 3pm PT

eEye Digital Security®

Security Landscape - *More than a Microsoft World*

- CTO/CSO/CxO News
  - Uncle Sam: If It Ends in .Com, It's .Seizable
  - Should US intelligence agency have a role in protecting electric grid?
  - Social Engineer Gets into RSA Conference for Free
  - Juniper buys web security company for $80 million
- IT Admin News
  - Windows 8 Kill Switch
  - Chrome Adopted As US State Department "Alternative" Certified Browser
  - Chinese Spy on NATO Officials using Facebook
- Researcher News
  - IE10 ForceASLR
  - Final Conclusion to the LulzSec Story
  - Duqu Mystery Language
  - Vulnerability in AMD CPUs causes Stack Corruption

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

- Demos, Guides, Whitepapers, Videos, Webinars, Events

→Contact Us

1.866.339.3732 or research@eEye.com

eEye Digital Security®