



eEye Digital Security[®]

Know your vulnerabilities. Know you're protected.

Vulnerability Expert Forum

January 11, 2012

Agenda

- About eEye
- Microsoft's January 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.”



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



→ “eEye’s security research team continues to provide good Windows vulnerability coverage and mitigation advice for zero-day vulnerabilities.”



→ “Retina has many desirable features...and an extremely flexible reporting portal. The product is also attractively priced.”



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 January Security Bulletins

→ 7 Total Bulletins; 8 Issues Fixed

- Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)
- Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)
- Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524)
- Vulnerabilities in Windows Media Could Allow Remote Code Execution (2636391)
- Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)
- Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)
- Vulnerability in AntiXSS Library Could Allow Information Disclosure (2607664)



eEye Digital Security®

Microsoft Security Bulletin: MS12-001

→ 1 Vulnerability Fixed in Bulletin

- CVE-2012-0001 - Windows Kernel SafeSEH Bypass Vulnerability

→ Severity: Important

→ Not so SafeSEH

- Bypasses SafeSEH defense-in-depth measures
- Issue has to do with where the Kernel loads the SEH tables

→ Mitigations

- Recompile software using a newer version of Microsoft Visual C++
- Enable Structured Exception Handling Overwrite Protection (SEHOP)



eEye Digital Security®

Microsoft Security Bulletin: MS12-002

- 1 Vulnerability Fixed in Bulletin
 - CVE-2012-0009 - Object Packager Insecure Executable Launching Vulnerability
- Severity: Important
- Windows Object Packager is out of control you guys...
 - Embedded packaged object
 - Must be triggered in the same directory as a malicious executable
 - Legitimate file is the vehicle for the exploit, not the exploit itself
- Mitigations
 - Disable the WebClient service
 - Block TCP ports 139 and 445 at the firewall
 - Register packager.exe with a full path



eEye Digital Security®

Microsoft Security Bulletin: MS12-003

- 1 Vulnerability Fixed in Bulletin
 - CVE-2012-0005 - CSRSS Elevation of Privilege Vulnerability
- Severity: Important
- CSRSS EoP FTL
 - Attacker must be local to the target machine
 - Only systems configured with Chinese, Japanese or Korean system locale are vulnerable
 - Specially crafted Unicode can trigger the vulnerability
- Mitigations
 - No reasonable mitigations at this time



eEye Digital Security®

Microsoft Security Bulletin: MS12-004

- 2 Vulnerabilities Fixed in Bulletin
 - CVE-2012-0003 - MIDI Remote Code Execution Vulnerability
 - CVE-2012-0004 - DirectShow Remote Code Execution Vulnerability
- Severity: Critical
- Media Player Serves Up More Than Just Music
 - Affects XP to W7
 - Specially crafted media files could allow for RCE
- Mitigations
 - Disable MIDI parsing
 - Disable the Line21 DirectShow filter



eEye Digital Security®

Microsoft Security Bulletin: MS12-005

- 1 Vulnerability Fixed in Bulletin
 - CVE-2012-0013 - Assembly Execution Vulnerability
- Severity: Important
- Tell that Packager to be cool! Say “Packager be cool!”
 - Another “embedded object” issue
 - Affects any format that can have embedded objects, such as .rtf, .doc, .pptx etc. etc.
 - Will not prompt before execution, “Application Launching” window may appear
- Mitigations
 - Remove the .application file association



eEye Digital Security®

Microsoft Security Bulletin: MS12-006

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-3389 - SSL and TLS Protocols Vulnerability
- Severity: Important
- The BEAST Returns
 - Addresses CBC issues with SSL 3.0\TLS 1.0
- Mitigations
 - Prioritize the RC4 Algorithm in server software on systems running Windows Vista, Windows Server 2008, Windows 7, or Windows Server 2008 R2
 - Enable TLS 1.1 and/or 1.2 in client software on systems running Windows 7 or Windows Server 2008 R2
 - Enable TLS 1.1 in server software on systems running Windows 7 or Windows Server 2008 R2



eEye Digital Security®

Microsoft Security Bulletin: MS12-007

- 1 Vulnerability Fixed in Bulletin
 - CVE-2012-0007 - AntiXSS Library Bypass Vulnerability
- Severity: Important
- AntiXSS XSS'ed
 - Incorrectly sanitizes HTML
 - Improperly parses escape characters in CSS
 - Allows for arbitrary script execution
- Mitigations
 - No reasonable mitigations at this time



eEye Digital Security®

The HashDoS Incident - MS11-100

→ Origins

- Presented at the Chaos Communication Congress (CCC)
- Based on earlier works on Denial of Service conditions caused by Algorithmic Complexity Attacks

→ How does it all work?

- Web servers hash POST parameter names
- Most languages don't restrict the number of names or length of request by default
- Collisions cause the request handler in the server to work abnormally hard

→ Updates on the matter...

- Microsoft released out-of-cycle patch (MS11-100)
- Mitigations...



eEye Digital Security®

VEF Contest

- You must post a comment on the **“HashDoS Crashes Your New Year’s Eve Party (and your web server)”** blog post.
 - <http://blog.eeye.com>
 - We will select the best response
- You must post your comment on the eEye Blog by Friday 01/13/12 at 3pm PT
- Prize: Kindle Fire



eEye Digital Security®

Other Vendor Updates

- Adobe Reader and Acrobat (APSB12-01)
 - 6 memory-based vulnerabilities leading to code execution
 - Affecting versions prior to 10.1.2 and 9.5 on Windows and Mac
- OpenSSL (SECADV-20120104)
 - 6 vulnerabilities leading to plain-text recovery, memory content disclosure, denial of service, or double-free condition
 - Affecting versions prior to 1.0.0f and 0.9.8s
- HP Printers and Digital Senders (CVE-2011-4161)
 - Design flaw in device Remote Firmware Update (RFU) does not verify digital signatures allowing unauthenticated arbitrary firmware installation
 - Affects numerous devices



eEye Digital Security®

Security Landscape - *More than a Microsoft World*

- CTO/CSO/CxO News
 - Android Malware Victims Offered Free Windows Phones
 - HP, IBM, MS Patching Laggards

- IT Admin News
 - The “Missing” 14th Bulletin
 - Windows 8 Refresh\Reset Button

- Researcher News
 - Hackers Get Symantec Anti-Virus Source Code
 - Using Encrypted Data without Decrypting It



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®