



eEye Digital Security[®]

Know your vulnerabilities. Know you're protected.

Vulnerability Expert Forum

December 14, 2011

Agenda

- About eEye
- Microsoft's 13 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 13 Security Bulletins

→ ~~14~~ 13 Total Bulletins; 19 Issues Fixed

- Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)
- Vulnerability in Microsoft Office IME (Chinese) Could Allow Elevation of Privilege (2652016)
- Vulnerability in Microsoft Office Could Allow Remote Code Execution (2590602)
- Cumulative Security Update of ActiveX Kill Bits (2618451)
- Vulnerabilities in Microsoft Publisher Could Allow Remote Code Execution (2607702)
- Vulnerability in Windows Media Could Allow Remote Code Execution (2648048)



eEye Digital Security®

Microsoft 13 Security Bulletins

- Vulnerability in OLE Could Allow Remote Code Execution (2624667)
- Vulnerabilities in Microsoft PowerPoint Could Allow Remote Code Execution (2639142)
- Vulnerability in Active Directory Could Allow Remote Code Execution (2640045)
- Vulnerability in Microsoft Excel Could Allow Remote Code Execution (2640241)
- Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712)
- Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171)
- Cumulative Security Update for Internet Explorer (2618444)



eEye Digital Security®

Microsoft Security Bulletin: MS11-087

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-3402 - TrueType Font Parsing Vulnerability
- Severity: Critical
- On the 1st Patch of Tuesday MS Gave to Me, 1 Duqu Vulnerability
 - Publicly reported with exploitation seen in-the-wild
 - Specially crafted TrueType Font within a document via web, e-mail, and file shares
 - High likelihood for exploits leveraging this flaw
- Mitigations
 - Restrict access to t2embed.dll
 - Block attack vectors (WebDAV, WebClient, NetBIOS ports)

Microsoft Security Bulletin: MS11-088

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-2010 - Pinyin IME Elevation Vulnerability
- Severity: Important
- Least Privilege, Lost in Translation
 - Privately reported
 - Design flaw
 - Local privilege elevation using MSPY IME toolbar
 - Code execution with system-level privileges
- Mitigations
 - None available



eEye Digital Security®

Microsoft Security Bulletin: MS11-089

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-1983 - Word Use After Free Vulnerability
- Severity: Important
- Say Word, Son
 - Privately reported
 - Parsing a crafted Word file causes a freed object to be reused, leading to memory corruption
 - Shared component
- Mitigations
 - Do not open Word files from untrusted sources or those unexpectedly received from trusted sources



eEye Digital Security®

Microsoft Security Bulletin: MS11-090

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-3397 - Microsoft Time Remote Code Execution Vulnerability
- Severity: Critical
- Datime Pwns You
 - Privately reported
 - A specially crafted (TIME) binary behavior could corrupt system state
 - Third-party kill-bits
- Mitigations
 - Disable TIME behavior
 - Prevent binary behaviors in Internet Explorer (a la kill bit)



eEye Digital Security®

Microsoft Security Bulletin: MS11-091

→ 4 Vulnerabilities Fixed in Bulletin

- CVE-2011-1508 - Publisher Function Pointer Overwrite Vulnerability
- CVE-2011-3410 - Publisher Out-of-bounds Array Index Vulnerability
- CVE-2011-3411 - Publisher Invalid Pointer Vulnerability
- CVE-2011-3412 - Publisher Memory Corruption Vulnerability

→ Severity: Important

→ Jingle Shells, Jingle Shells

- 1 Publicly Released, 3 Privately Reported
- Improper handling of memory values and memory for function pointers
- Prime holiday card vulnerabilities

→ Mitigations

- Do not open Publisher files from untrusted sources or those unexpectedly received from trusted sources



eEye Digital Security®

Microsoft Security Bulletin: MS11-092

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-3401 - Windows Media Player DVR-MS Memory Corruption Vulnerability
- Severity: Critical
- SBE = SBD
 - Privately reported
 - Crafted DVR-MS files
 - Code execution in context of user running Media Player / Media Center
- Mitigations
 - Restrict access to encdec.dll, or unregister encdec.dll
 - Avoid opening .dvr-ms files from untrusted sources



eEye Digital Security®

Microsoft Security Bulletin: MS11-093

→ 1 Vulnerability Fixed in Bulletin

- CVE-2011-3400 - OLE Property Vulnerability

→ Severity: Important

→ OLE Strikes Again

- Privately reported
- Improper handling of OLE objects in memory
- Document containing crafted OLE object
- Office files, third-party file types, e-mail attachments
- Remote code execution

→ Mitigations

- Do not open files from untrusted sources or those unexpectedly received from trusted sources



eEye Digital Security®

Microsoft Security Bulletin: MS11-094

→ 2 Vulnerabilities Fixed in Bulletin

- CVE-2011-3396 - PowerPoint Insecure Library Loading Vulnerability
- CVE-2011-3413 - OfficeArt Shape RCE Vulnerability

→ Severity: Important

→ Your Art Was the Prettiest Art of All the Art

- Both Privately Reported
- PowerPoint file containing crafted OfficeArt record
- You guessed it! DLL Hijacking!

→ Mitigations

- Block attack vectors (WebDAV, WebClient, NetBIOS ports)
- Enable Office File Block Policy for binary files
- Enable Microsoft Office Isolated Conversion Environment (MOICE) for Office files



eEye Digital Security®

Microsoft Security Bulletin: MS11-095

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-3406 - Active Directory Buffer Overflow Vulnerability
- Severity: Important
- Buffer Overflow, Missing you. Yours, Active Directory
 - Privately reported
 - Specially crafted query causes a buffer overflow
 - Code execution in context of the Network Service account
 - Requires credentials to AD domain
- Mitigations
 - Block inbound and outbound traffic for TCP port 389 at perimeter firewalls to deter potential exploitation



eEye Digital Security®

Microsoft Security Bulletin: MS11-096

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-3403 - Record Memory Corruption Vulnerability
- Severity: Important
- Yet Another Office Vulnerability
 - Privately reported
 - Affects Excel 2003 SP3 and Office 2004 for Mac
 - Excel file containing crafted record object
 - Remote code execution
- Mitigations
 - Enable Office File Validation
 - Enable Office File Block Policy for binary files
 - Enable Microsoft Office Isolated Conversion Environment (MOICE) for Office files



eEye Digital Security®

Microsoft Security Bulletin: MS11-097

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-3408 - CSRSS Local Privilege Elevation Vulnerability
- Severity: Important
- It's Beginning to Look a Lot Like Rootkit
 - Privately reported
 - Improper validation of device event message permissions between low-integrity processes and high-integrity processes
- Mitigations
 - None available



eEye Digital Security®

Microsoft Security Bulletin: MS11-098

- 1 Vulnerability Fixed in Bulletin
 - CVE-2011-2018 - Windows Kernel Exception Handler Vulnerability
- Severity: Important
- Kernels Roasting on an Open Fire
 - Privately reported
 - Improper initialization of objects in memory
 - Elevation of privilege
- Mitigations
 - None Available



eEye Digital Security®

Microsoft Security Bulletin: MS11-099

→ 3 Vulnerabilities Fixed in Bulletin

- CVE-2011-1992 - XSS Filter Information Disclosure Vulnerability
- CVE-2011-2019 - Internet Explorer Insecure Library Loading Vulnerability
- CVE-2011-3404 - Content-Disposition Information Disclosure Vulnerability

→ Severity: Important

→ IE Got Run Over By A Reindeer

- All privately reported
- Content disclosure between different domains or IE Zones
- DLL Hijacking

→ Mitigations

- Block or configure to prompt on ActiveX and Active Scripting in Internet and Local intranet security zones
- Block attack vectors (WebDAV, WebClient, NetBIOS ports)



eEye Digital Security®

Microsoft Security Bulletin: MS11-010

→ “Missing” Bulletin

- CVE-2011-3389 - Vulnerability in SSL/TLS Could Allow Information Disclosure

→ “BEAST” Attack

- Microsoft Security Response Center (MSRC) reported that the “missing” bulletin would have addressed the issue discussed Microsoft Security Advisory 2588513



eEye Digital Security®

VEF Contest

- You must read the **“Security Predictions: All Hat, No Cattle”** blog and post your prediction in the “Comments” section:
 - New threats in 2012
 - How business usage of technology will evolve in 2012
- We will select the best prediction in each category
- Post your comment on the eEye Blog (<http://blog.eeye.com>) by Friday 12/16/11 at 3pm PT
- Prize: Amazon Kindle + \$25 Amazon gift card



eEye Digital Security®

Security Landscape - *More than a Microsoft World*

→ CTO/CSO/CxO News

- Survey: Mobile, Virtualization Biggest Security Challenge
- SOPA
- Water Utility Damaged by Cyberattack?

→ IT Admin News

- Flash to HTML5 conversion Tool
- C|Net Download.Com bundling Nmap with malware
- Verizon Cites Security Issue for Nixing Google Wallet

→ Researcher News

- Android Malware Infection Growth Rate
- Google Pushing Forward Secrecy
- Google Proposes SSL System Fix
- The One Ring to Rule Them All
- Android Fail



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®