



eEye Digital Security[®]

Know your vulnerabilities. Know you're protected.

Vulnerability Expert Forum

November 9, 2011

Agenda

- About eEye
- Microsoft's November Security Bulletins
- Other Vendor Updates
- 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 November Security Bulletins

→ 4 Total Bulletins; 4 Issues Fixed

- Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)
- Vulnerability in Windows Kernel-Mode Drivers Could Allow Denial of Service (2617657)
- Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)
- Vulnerability in Active Directory Could Allow Elevation of Privilege (2630837)



eEye Digital Security®

Microsoft Security Bulletin: MS11-083

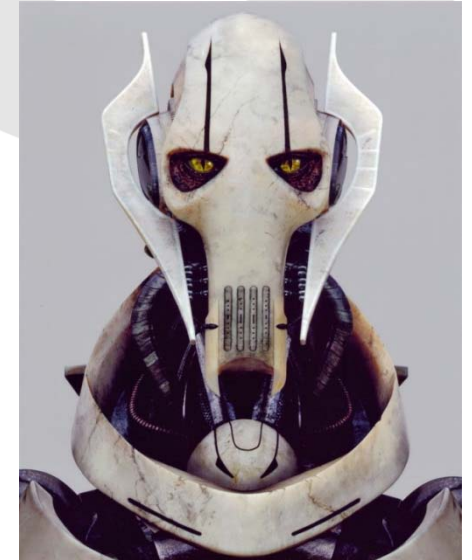
- 1 Vulnerability Fixed in Bulletin
 - Reference Counter Overflow Vulnerability - CVE-2011-2013
- Severity: Critical
- Just when you thought you were safe...
 - Privately reported
 - Specially crafted UDP packets to a closed port can cause counter overflow
 - High likelihood for attempts to create exploits leveraging this flaw
 - DoS > RCE
- Mitigations
 - Block unused UDP ports at the perimeter firewall
 - Don't panic!



eEye Digital Security®

Microsoft Security Bulletin: MS11-084

- 1 Vulnerability Fixed in Bulletin
 - TrueType Font Parsing Vulnerability - CVE-2011-2004
- Severity: Moderate
- Not quite Duqu
 - Privately reported
 - Specially crafted TrueType file via WebDAV, email
 - High likelihood for exploits leveraging this flaw
- Mitigations
 - Disable WebClient service
 - Block TCP ports 139 and 445 at the firewall



General Grievous,
apprentice of Count
Duqu



eEye Digital Security®

Microsoft Security Bulletin: MS11-085

- 1 Vulnerability Fixed in Bulletin
 - Windows Mail Insecure Library Loading Vulnerability - CVE-2011-2016
- Severity: Important
- **BREAKING NEWS: DLL Preloading Issue Found in Windows Mail**
 - Privately reported
 - Affects .eml and .wcinv file loading
- Mitigations
 - Disable loading of libraries from WebDAV
 - Disable WebClient
 - Block TCP ports 139 and 445



eEye Digital Security®

Microsoft Security Bulletin: MS11-086

→ 1 Vulnerability Fixed in Bulletin

- LDAPS Authentication Bypass Vulnerability - CVE-2011-2014

→ Severity: Important

→ LDAPSSL

- Privately reported
- Affects Active Directory, Active Directory Application Mode (ADAM), and Active Directory Lightweight Directory Service (AD LDS)
- Elevation of privilege via LDAP over SSL, attacker can use revoked certificate to authenticate to the AD

→ Mitigations

- Remove any compromised user accounts (those using the revoked certificate) from domain
- IPsec-based connections in “Always check CRL” mode



eEye Digital Security®

VEF Contest

- You must post a comment on the **“Duqu, Son of Stuxnet, Destroyer of Worlds!”** blog post.
 - <http://blog.eeye.com>
 - We will pick someone from the responses posted
- You must post your comment on the eEye Blog by Friday 11/11/11 at 3pm PT
- Prize: Amazon Kindle + \$25 Amazon gift card



eEye Digital Security®

Oracle - CPU-OCT-2011

→ 57 Vulnerabilities Fixed

- Affecting Database, Fusion Middleware, E-Business Suite, Supply Chain, PeopleSoft, Siebel, Industry Applications, Sun Product Suite, Linux Product Suite, and Virtualization

→ Database

- 5 vulnerabilities across Oracle Net and HTTP with most severe potentially allowing code execution (CVSS 8.5 – “complete” C/I/A)
- None are remotely exploitable without authentication
- Do not affected client installs (only Database server)

→ Fusion Middleware

- 10 vulnerabilities across HTTP and local Outside In Filters with most severe impacts affecting “partial” C/I/A and “partial+” C/I
- 5 remotely exploitable without authentication
- Include Database components



eEye Digital Security®

Oracle - CPU-OCT-2011 (Cont.)

→ “Applications”

- 5 vulnerabilities across E-Business Suite HTTP services with the most severe affecting “partial” integrity and 3 being remotely exploitable
- 1 remote vulnerability in Supply Chain HTTP affecting “partial” integrity
- 7 vulnerabilities in PeopleSoft products across HTTP with 4 affecting “partial” confidentiality and integrity
- 3 vulnerabilities in Siebel CRM across HTTP with 1 vulnerability being remotely exploitable and the most severe affecting “partial” confidentiality and integrity

→ Industry Applications

- 2 vulnerabilities across HTTP services, both remotely exploitable without authentication affecting “partial” integrity

→ Linux Products

- 1 vulnerability in Oracle validated subcomponent with impact affecting “partial” confidentiality/integrity

→ Virtualization Products

- 1 vulnerability in Sun Ray TCP/IP authentication subcomponent with impact affecting “partial” C/I/A



eEye Digital Security®

Oracle Sun - CPU-OCT-2011

→ 22 Vulnerabilities Fixed

- Glassfish Server, Oracle Communications Unifid, Oracle OpenSSO, Oracle Waveset, Solaris, and SPARC T3, Netra SPARC T3, Sun Fire, and Sun Blade

→ Solaris

- 15 vulnerabilities spanning procs, Kernel, ZFS, xscreensaver, libdtrace, Zones, LDAP library iSCSI Datamover, statd, rquotad, libnsl
- Most severe of vulnerabilities in LDAP library being remotely exploitable without authentication potentially leading to arbitrary code execution (CVSS 9.3)

→ Glassfish

- Remote vulnerability in HTTP affecting “complete” availability

→ OpenSSO

- 2 remote vulnerabilities in HTTP with most severe impact affecting  “complete” availability

eEye Digital Security®

Oracle Sun - CPU-OCT-2011 (cont.)

→ Waveset

- Remote vulnerability in HTTP with impact affecting “partial” confidentiality, integrity, and availability (C/I/A)

→ Communications Unified

- 2 remote vulnerabilities in multiple protocols with most severe impact affecting “partial” integrity

→ SPARC T3, Netra SPARC T3, Sun Fire, Sun Blade

- Vulnerability in Integrated Lights Out Manager CLI that could affect “partial” confidentiality



eEye Digital Security®

VMware - VMSA-2011-0013

→ 64 Vulnerabilities Fixed

- Affecting third-party components: OpenSSL, libuser, nss, nspr, JRE 1.6, JRE 1.5, SFCB

→ VMware vCenter Server, vCenter Update Manager, ESXi, and ESX

→ OpenSSL updates

- Disclosure of sensitive information (force cipher downgrade)
- ESX 4.1: Apply ESX410-201110204-SG
- ESX 4.0: Patch is pending

→ Libuser updates

- Default password for LDAP based accounts
- ESX 4.1: Apply ESX410-201110206-SG
- ESX 4.0: Patch is pending



eEye Digital Security®

VMware - VMSA-2011-0013 (Cont.)

→ Service Console nss and nspr updates

- MITM attacks leading to spoofing of arbitrary SSL servers
- Brute-force attacks against cryptographic protection mechanisms
- ESX 4.1: Apply ESX410-201110214-SG
- ESX 4.0: Patch is pending

→ JRE 1.5/1.6 updates

- Multiple vulnerabilities with most severe leading to code execution
- JRE 1.6: Fixes from Update 24 (Feb 2011) and Update 22 (Oct 2010)
- JRE 1.5: Fixes from Update 30 (Jun 2011) and Update 28 (Feb 2011)
- vCenter 4.1 and Update Manager 4.1: Apply Windows Update 2
- ESX 4.1: Apply ESX410-201110201-SG
- vCenter 4.0, VirtualCenter 2.5, Update Manager 4.0, ESX 4.0, and ESX 3.5: Patches are pending
- ESX 3.0.3: No patches are planned



eEye Digital Security®

Other updates...



eEye Digital Security®

Security Landscape - *More than a Microsoft World*

→ CTO/CSO/CxO News

- The 11% That Get Security
- US Intelligence Group Wants To Change The Way Chips Are Made
- What Keeps Fed CIOs Busy? Infosec

→ IT Admin News

- New Attack Campaign Launched With Blackhole
- The End Of An Era: Internet Explorer Drops Below 50% Of Web Usage
- Anyone With A Smart Cover Can Break Into Your iPad 2

→ Researcher News

- Android Orphans: Visualizing A Sad History Of Support
- Lethal Medical Device Hack Taken To Next Level
- Duqu Trojan Questions And Answers
- Feds Concerned About Hackers Opening Prison Doors



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 Unified Vulnerability Management

MANAGE AND REPORT

- End-to-end vulnerability and compliance management
- Centralized management, reporting, and controls
- Assess, mitigate, and protect from one console
- Advanced trending and analytics

ASSESS

- Vulnerability Scanning
- Configuration Auditing
- Asset Discovery & Inventory
- Zero-Day Vulnerability Identification
- Vulnerability Reporting
- Compliance Auditing

MITIGATE

- Integrated Patch Management
- Prioritized Mitigation
- Risk Scoring
- Security Alerts
- Prescriptive Remediation Reporting

PROTECT

- Zero-Day Protection
- Intrusion Prevention
- Web Protection
- Application Protection
- System Protection

SECURITY RESEARCH



Automation and Efficiency = Minimized Risk and 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®