

Minimize the Impact of Patch Tuesday

Wednesday, June 9th 2010

For audio, please call 1 (888) 268-4178

Intl: +1 617 597 5494

code: 94883955

Presented by
Jason Miller
Jace Mclean

Sponsored By:

Shavlik

- Offers the simplest way to secure complex enterprise networks.
 - Active Vulnerability Management maintains secure, policy-compliant configurations through automatic and continuous Assessment, Remediation and Management.

Patch Management.org

- The industry's first mailing list dedicated to the discussion of patch management.
- www.patchmanagement.org

Logistics

- Feel free to ask questions via the online Q&A link in the Live Meeting interface
 - Questions may be answered during the presentation
 - Unanswered questions will be resolved via email after the presentation is over
 - ***When asking a question, please include your email address so we can answer you offline if we run out of time***
- A copy of this presentation is available for download within the Live Meeting application

Agenda

- Review June Security Bulletins
- June 2010 Shavlik Patch Recommendation
- Other items from June Patch Tuesday
- Other patches released since last patch day
- Outstanding vulnerabilities and advisories

Overview for June 2010

- 10 Microsoft Security Bulletins / 34 Vulnerabilities Addressed
- Affected Products
 - 6 bulletins affect Operating Systems
 - 2 bulletins affect Office
 - 1 bulletin affects Internet Explorer
 - 1 bulletin affects OS and Office
- Maximum Severity / Impact Rating Breakdown
 - 3 bulletins rated as Critical
 - 7 bulletins rated as Important
 - 6 bulletins can lead to Remote Code Execution
 - 3 bulletins can lead to Elevation of Privilege
 - 1 bulletin can lead to Tampering

... continued

... continued: Overview for June 2010

- Exploitability Rating Breakdown
 - 6 bulletins have Exploitability Index 1: Consistent exploit code likely
 - 2 bulletins have Exploitability Index 2: Inconsistent exploit code likely
 - 1 bulletin has Exploitability Index 3: Functioning exploit code unlikely
 - 1 bulletin has no Exploitability Index rating
- Apple Safari 4.1 and 5.0

Bulletin Agenda

- MS10-032 – Windows Kernel
- MS10-033 – Windows Media
- MS10-034 – ActiveX Kill Bits
- MS10-035 – Internet Explorer
- MS10-036 – Microsoft Office (COM)
- MS10-037 – OpenType Compact Font
- MS10-038 – Microsoft Office
- MS10-039 – Microsoft
- MS10-040 – IIS
- MS10-041 – .NET Framework

MS10-032: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)

- Important
- Applies to all supported Microsoft Operating Systems
- Can lead to Elevation of Privilege on machine
- Attacker must first log on to system to carry out attack
- Attacker runs specially crafted program allowing complete control over system
- No notes of patch looking for abnormalities like previous updates
- ***Test patch before deploying***
- Fixes 3 vulnerabilities, 2 publically known, no reports of attacks
- Replaces MS09-065 on Windows 2000, XP, 2003, Vista and 2008, does not replace any previous security bulletins on Windows 7 and 2008 R2
- Exploitability Index: 1 - Consistent exploit code likely

MS10-033: Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)

- Critical
- Applies to all supported Microsoft Operating Systems
- Affects DirectShow, Windows Media Format Runtime: 9, 9.5, 11; Windows Media Encoder 9, COM component (Asycfilt.dll)
- Open maliciously crafted media file (MPEG, ASF, WMA) can lead to Remote Code Execution
- Media can be downloaded from web or email, or streaming format
- **Multiple patches can show missing on single machine for this bulletin
- Fixes 2 vulnerabilities, none publically known, no reports of attacks
- Replaces MS09-028 for DirectShow, MS09-047 for Media Format Runtime, does not replace previous bulletins for some installations
- Exploitability Index: 1 - Consistent exploit code likely

MS10-034: Cumulative Security Update of ActiveX Kill Bits (980195)

- Critical
- Applies to all supported Microsoft Operating Systems
- Blocks Microsoft Data Analyzer ActiveX
 - ActiveX control not installed on default Office installations, must be installed manually
- Blocks Microsoft Internet Explorer 8 Developer Tools ActiveX
- Blocks third party ActiveX controls: Danske Bank, CA's Pest Scan, Eastman Kodak Company's Ofoto Upload Manager, Avaya's CallPilot Unified Messaging.
- Fixes 2 vulnerabilities, none publically known, no reports of attacks
- Replaces security bulletin MS10-008
- No Exploitability Index rating

MS10-035: Cumulative Security Update for Internet Explorer (982381)

- Critical
- Affects all supported versions of Internet Explorer
- Visit malicious website can lead to Remote Code Execution
- Addresses issue in Security Advisory KB980088
- Un-apply workaround before patching
- Contains defense-in-depth update for IE 8 XSS filter
- Fixes Pwn2Own contest vulnerability
- Update offered to IE 5.01 SP4 to fix regression problem from MS09-054: download dialog may become unresponsive
- Fixes 5 vulnerabilities, none publically known, no reports of attacks
- Replaces security bulletin MS10-018
- Exploitability Index: 1 - Consistent exploit code likely

MS10-036: Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)

- Important
- Applies Office XP**, 2003***, 2007***; Excel, PowerPoint, Publisher, Visio, Word.
- Open specially crafted document can lead to remote code execution
- **Office XP SP3 is vulnerable, but no patch is being supplied.
 - Patch deemed “infeasible”
 - Remove Office XP SP3 or upgrade to Office 2003, 2007 or 2010
 - Microsoft supplying FixIt tool to add defense on XP: KB983235
- ***If patching standalone Office product, the full Office patch must be installed as well for Office 2003 or Office 2007

...continued

... continued: MS10-036: Vulnerability in COM Validation in Microsoft Office Could Allow Remote Code Execution (983235)

- Fixes 1 vulnerability, not publically known, no reports of attacks
- Replaces multiple security bulletins: please refer to bulletin
- Exploitability Index: 1 - Consistent exploit code likely

MS10-037: Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)

- Important
- Applies to all supported Microsoft Operating Systems
- Attacker must first log on to system to carry out attack
- Attacker runs specially crafted program allowing complete control over system
- Fixes 1 vulnerability, not publically known, no reports of attacks
- Does not replace any previous security bulletins
- Exploitability Index: 2 - Inconsistent exploit code likely

MS10-038: Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)

- Important
- Applies Excel 2002, 2003, 2007; Excel Viewer 2007, Office Compatibility Pack 2007
- Fixes in MS10-036 for Excel 2003 and 2007 are addressed in this bulletin as well. Only MS10-036 or MS10-038 needs to be applied (no need to apply both updates)
- Open specially crafted document can lead to Remote Code Execution
- Fixes 14 vulnerabilities, none publically known, no reports of attacks
- Replaces security bulletin MS10-017
- Exploitability Index: 1 - Consistent exploit code likely

MS10-039: Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (2028554)

- Important
- Applies InfoPath 2003, 2007; SharePoint Server 2007, SharePoint Services 3.0
- Addresses issue in Security Advisory KB983438
- Clicking on specially crafted link can result in Elevation of Privilege on SharePoint server session (not client system)
- Related to MS10-035 (IE). Both bulletins address same vulnerability (toStaticHTML). Both patches must be applied as each fixes different software (IE vs. SharePoint)
- Fixes 3 vulnerabilities, 1 publically known, 1 has reports of attacks
- Replaces MS08-077 (SharePoint Server 2007 only)
- Exploitability Index: 1 - Consistent exploit code likely

MS10-040: Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)

- Important
- Applies to IIS 6.0, 7.0. 7.5 on Windows 2003, Vista, 2008, 7, 2008 R2***
- Windows Vista, 2003 and 2008 are only vulnerable if Extended Protection for Authentication (KB973917) has been applied
- IIS server receiving specially crafted HTTP request can result in remote code execution
- IIS server must be configured to support authentication requests using EPA only. This is not the default configuration for IIS
- Fixes 1 vulnerability, not publically known, no reports of attacks
- Does not replace any previous security bulletins
- Exploitability Index: 2 - Inconsistent exploit code likely

MS10-041: Vulnerability in Microsoft .NET Framework Could Allow Tampering (981343)

- Important
- Applies to .NET 1.0, 1.1, 2.0, 3.5 on all supported operating systems
- Attacker sends specially crafted XML can result in Tampering
- Tampering: malicious modification of data such as data or information flow between two computers.
- Fixes 1 vulnerability, publically known, no reports of attacks
- Replaces multiple security bulletins: please refer to bulletin
- Exploitability Index: 3 - Functioning exploit code unlikely

June 2010 Recommendations

- Patch MS10-033 (Windows Media) and MS10-035 (IE) first
- Deploy remaining patches
 - Safari

Other items from June Patch Tuesday

- Security Advisory 973811 Updated:
 - Extended Protection for Authentication now covers .NET Framework
- No previous security patches re-released
- Apple Safari 4.1 / 5.0
 - Addresses 47 vulnerabilities
 - Safari 4.1 Mac OS only, Safari 5.0 Windows and Mac OS
- Adobe announces upcoming security bulletin releases
 - Adobe Flash 10: June 10
 - Adobe Reader and Acrobat: June 29

Other Items Since Last Patch Tuesday

- No major releases from MS and Non-MS vendors

Outstanding Vulnerabilities and Advisories

- ~~Security Advisory 983438 (April 29, 2010) – Expired with MS10-039~~
- ~~Security Advisory 980088 (February 03, 2010) – Expired with MS10-035~~
- Microsoft Security Advisory 977377 (February 10, 2010)
 - Vulnerability in TLS/SSL Could Allow Spoofing

Contact Information:

- Email: webinars@shavlik.com
- Shavlik Technical Support: support@shavlik.com, 800-690-6911
- Domestic Sales: sales@shavlik.com, 800-690-6911
- International Sales: international@shavlik.com, +1 (612) 331-6737
- Security Center Blog: <http://securitycenterblog.shavlik.com/>
- Shavlik XML on Twitter: <http://twitter.com/shavlikxml>



Simply Secure.