



shavlik

**Minimize the Impact of Patch Tuesday  
Wednesday, August 11th 2010**

For audio, please call 1 (888) 268-4178  
Intl: +1 617 597 5494  
code: 94883955

Presented by  
Jason Miller  
Jace Mclean

## Sponsored By:



- Provides cloud-based software for simplifying and automating IT operations, enabling organizations to verify, secure and manage their physical and virtual cloud IT assets.



- The industry's first mailing list dedicated to the discussion of patch management.
  - [www.patchmanagement.org](http://www.patchmanagement.org)

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

For audio, please call 1 (888) 268-4178 code: 94883955

## Overview for August 2010



- 14 Microsoft Security Bulletins / 34 Vulnerabilities Addressed
  - Most bulletins released at one time on a patch Tuesday
  - Tied most vulnerabilities in one patch Tuesday (June 2010)
- Affected Products
  - 10 bulletins affect Operating Systems
  - 2 bulletins affect Office, 1 bulletin affects Silverlight, 1 bulletin affects Internet Explorer
- Maximum Severity / Impact Rating Breakdown
  - 8 bulletins rated as Critical
  - 6 bulletin rated as Important
  - 10 bulletins can lead to Remote Code Execution
  - 4 bulletins can lead to Elevation of Privilege
- Exploitability Rating Breakdown
  - 11 bulletins have Exploitability Index 1: Consistent exploit code likely
  - 3 bulletins have Exploitability Index 2: Inconsistent exploit code likely

For audio, please call 1 (888) 268-4178 code: 94883955

## Bulletin Agenda



- MS10-047 – Kernel
- MS10-048 – Kernel-Mode
- MS10-049 – SChannel
- MS10-050 – Outlook
- MS10-051 – XML Core
- MS10-052 – MPEG-3
- MS10-053 – IE Cumulative
- MS10-054 – SMB
- MS10-055 – Cinepak Codec
- MS10-056 – Word

For audio, please call 1 (888) 268-4178 code: 94883955

## Bulletin Agenda Continued



- MS10-057 – Excel
- MS10-058 – TCP/IP
- MS10-059 – Tracing
- MS10-060 – Silverlight / .NET
- MS10-046 – Windows LNK (out-of-band)

For audio, please call 1 (888) 268-4178 code: 94883955

## MS10-047: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)



- Important
- Applies to Windows Kernel on Windows XP x86, Vista, 2008, 7, 2008 R2
- Attacker must log on to system in order to exploit vulnerability
- Windows XP x86, Vista, 2008 can lead to Elevation of Privilege
- Windows 7, 2008 R2 can lead to Denial Of Service
- Fixes 3 vulnerabilities, none publically known, no reports of attacks in wild
- Replaces previous security bulletin MS10-021
- Exploitability Index: 1 - Consistent exploit code likely

## MS10-048: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)



- Important
- Applies to all supported Microsoft Operating Systems
- Attacker must log on to system in order to exploit vulnerability
- Attacker logs in to machine, runs specially crafted program, can lead to Elevation of Privilege
- Fixes 5 vulnerabilities, 1 publically known (CVE-2010-1894), no reports of attacks in wild
- Replaces previous security bulletin MS10-032
- Exploitability Index: 1 - Consistent exploit code likely

For audio, please call 1 (888) 268-4178 code: 94883955

## MS10-049: Vulnerabilities in SChannel could allow Remote Code Execution (980436)



- Critical, Replaces Security Advisory 977377
- Applies to all supported Microsoft Operating Systems
- Visiting malicious secure (https) website with man-in-the-middle attack could lead to Remote Code Execution.
- Most likely scenario is Denial Of Service due to difficulty of attack
- Multivendor issue, more vendors should be releasing updates soon
- Fixes 2 vulnerabilities, 1 publically known(CVE-2009-3555), no reports of attacks in wild
- Does not replace any previous security bulletins
- Exploitability Index: 2 - Inconsistent exploit code likely

For audio, please call 1 (888) 268-4178 code: 94883955

## MS10-050: Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (981997)



- Important
- Applies to Movie Maker 2.1, 2.6, 6.0 on Windows XP and Vista
- Movie Maker 2.1 is installed by default on Windows XP and Vista
- Opening specially crafted Windows Movie Maker file could lead to Remote Code Execution
- Fixes 1 vulnerability, not publically known, no reports of attacks in wild
- Replaces previous security bulletin MS10-016
- Exploitability Index: 1 - Consistent exploit code likely

## **MS10-051: Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)**



- Critical
- Applies to XML Core Services 3.0 on all supported operating systems
- Visiting malicious website through Internet Explorer that invokes MSXML could lead to Remote Code Execution
- Difficult to perform exploit for attacker
- Fixes 1 vulnerability, not publically known, no reports of attacks in wild
- Replaces previous security bulletin MS08-069 on some operating systems
- Exploitability Index: 2 - Inconsistent exploit code likely

## MS10-052: Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)



- Critical
- Applies to Windows XP and 2003
- Opening specially crafted streaming file (ASX) or opening specially crafted media file could result in Remote Code Execution
- Popular form of media, likely to see attacks soon
- Fixes 1 vulnerability, not publically known, no reports of attacks in wild
- Does not replace any previous security bulletins
- Exploitability Index: 1 - Consistent exploit code likely

## MS10-053: Cumulative Security Update for Internet Explorer (2183461)



- Critical
- Applies to Internet Explorer 6, 7 and 8 on all supported operating systems (Internet Explorer 5 no longer supported with the end of life of Windows 2000)
- Visiting malicious website could lead to Remote Code Execution
- Internet Explorer 6 particularly at risk. Internet Explorer 7 and 8 would be difficult to program exploit
- Fixes 6 vulnerabilities, none publically known, no reports of attacks in wild
- Replaces previous security bulletin MS10-035
- Exploitability Index: 1 - Consistent exploit code likely

## MS10-054: Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)



- Critical
- Windows XP and 2003 can lead to Remote Code Execution
  - Higher severity due to unauthenticated attacks
- Windows Vista, 2008, 7 and 2008 R2 can lead to Elevation of Privilege
  - Lower severity due to authentication required for attacks
- Sending specially crafted SMB packet can lead to exploitation
  - Successful attack results are not controlled by attacker, controlled by target machine
  - Most likely scenario is a system stops responding, only one attack attempt before system crashes
- Fixes 3 vulnerabilities, none publically known, no reports of attacks in wild
- Replaces previous security bulletin MS10-012
- Exploitability Index: 2 - Inconsistent exploit code likely

For audio, please call 1 (888) 268-4178 code: 94883955

## MS10-055: Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)



- Critical
- Applies to Cinepak Codec on Windows XP, Vista and 7
- Codec installed by default on affected operating systems
- Opening specially crafted media file (AVI) can lead to Remote Code Execution
- Fixes 1 vulnerability, not publically known, no reports of attacks in wild
- Does not replace any previous security bulletins
- Exploitability Index: 1 - Consistent exploit code likely

## MS10-056: Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)



- Critical
- Applies to Word XP, 2003, 2007; Office Word Viewer (2007), Office Compatibility Pack 2007
- Opening specially crafted document (RTF) can lead to Remote Code Execution
- RTF Files typically not blocked by external email filters
- Outlook 2007 uses Word as preview pane for RTF files. Other versions of Outlook not affected.
- Fixes 4 vulnerabilities, none publically known, no reports of attacks in wild
- Replaces previous security bulletins: MS09-068, MS10-036, MS09-027
- Exploitability Index: 1 - Consistent exploit code likely

For audio, please call 1 (888) 268-4178 code: 94883955

## MS10-057: Vulnerability in Microsoft Office Excel Could Allow Remote Code Execution (2269707)



- Important
- Applies to Excel XP, 2003
- Opening specially crafted Excel file can lead to Remote Code Execution
- Rated Important as attacker gains rights as logged on user
- Fixes 1 vulnerability, not publically known, no reports of attacks in wild
- Replaces previous security bulletin MS10-036, MS10-038
- Exploitability Index: 1 - Consistent exploit code likely

## MS10-058: Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)



- Important
- Applies to IPv6 on Windows Vista, 2008, 7, 2008 R2
- Sending specially crafted IPv6 packet to machine can cause system to be unresponsive (DoS)
- Attacker logs in to machine, runs specially crafted program, can lead to elevation of privilege (x64 machines not affected by this vulnerability)
- Fixes 2 vulnerabilities, none publically known, no reports of attacks in wild
- Replaces previous security bulletin MS10-029, does not replace previous security bulletin on Windows 7 and 2008 R2
- Exploitability Index: 1 - Consistent exploit code likely

## MS10-059: Vulnerabilities in the Tracing Feature for Services Could Allow Elevation of Privilege (982799)



- Important
- Applies to Vista, 2008, 7 and 2008 R2
- Attacker must log on to system in order to exploit vulnerability
- Attacker logs in to machine, runs specially crafted program, can lead to elevation of privilege
- Fixes 2 vulnerabilities, 1 publically known (CVE-2010-2554), no reports of attacks in wild
- Does not replace any previous security bulletins
- Exploitability Index: 1 - Consistent exploit code likely

## MS10-060: Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)



- Critical
- Applies to .NET 2.0 and 3.5 on all supported Microsoft operating systems; Silverlight 2 and 3 on Windows server and clients
- Visiting malicious website could lead to Remote Code Execution
- Silverlight extremely easy to install, user base increasing, identify on network
- Fixes 2 vulnerabilities, none publically known, no reports of attacks in wild
- Replaces previous security bulletin MS09-061 on some operating systems for .NET, Does not replace any previous security bulletins for Silverlight
- Exploitability Index: 1 - Consistent exploit code likely

For audio, please call 1 (888) 268-4178 code: 94883955

## MS10-046: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198) – Out-Of-Band



- Critical
- Applies to all supported operating systems
- Removable drive contains malicious shortcut pointing to malware. User opens drive in Windows Explorer can lead to Remote Code Execution
- Malicious web site or remote network share contains malicious files. Windows attempts to load icon of shortcut triggering Remote Code Execution
- Fixes 1 vulnerability, 1 publically known (CVE-2010-2568), vulnerability attacked by a number of malware families
- Does not replace any previous security bulletins
- Exploitability Index: 1 - Consistent exploit code likely

For audio, please call 1 (888) 268-4178 code: 94883955

## August 2010 Recommendations



- Patch MS10-052 (MPEG-3), MS10-055 (Cinepak), MS10-056 (Word), MS10-060 (Silverlight, .NET) first
- Patch MS10-053 (IE), MS10-054 (SMB), MS10-057 (Excel) next
- Deploy remaining patches
- Adobe Flash and Microsoft Out-of-band release should be in your deployment cycle

## Other items from August Patch Tuesday



- Adobe Bulletin APSB10-016
  - Affects Adobe Flash Player 10.1.53.64, Adobe Flash Player 9.0.277.0, Adobe Air 2.0.2.12610
  - Fixes 6 vulnerabilities
  - Rated Critical
- Adobe Bulletin APSB10-019
  - Affects Flash Media Server 3.5.3 and Flash Media Server 3.0.5
  - Fixes 4 vulnerabilities
  - Rated Critical
- Adobe Bulletin APSB10-018
  - Affects ColdFusion 8.0, 8.0.1, 9.0 and 9.0.1
  - Fixes 1 vulnerability
  - Rated Important

For audio, please call 1 (888) 268-4178 code: 94883955

## Other items from August Patch Tuesday



- Microsoft Security Advisory 2264072
  - Elevation of Privilege Using Windows Service Isolation Bypass
  - Attack vector extremely rare
  - Microsoft not supplying a security update
  - Microsoft supplying non-security update: KB982316
  - Review bulletin for details

For audio, please call 1 (888) 268-4178 code: 94883955

## Other items since last Patch Tuesday



- Apple iTunes 9.2.1 - 7/19/2010
  - Fixes Critical vulnerability CVE-2010-1777
  - If you do not have QuickTime currently installed, the iTunes installer will install version 7.66.73.0. QuickTime version 7.66.71.0 is the version publically available on Apple's site
- Mozilla Firefox 3.5.11 - 7/20/2010
  - Security release fixing 11 issues
    - 7 Critical Vulnerabilities
    - 1 High Vulnerability
    - 3 Moderate Vulnerabilities
- Mozilla Firefox 3.6.7 - 7/20/2010
  - Security release fixing 14 issues
    - 8 Critical Vulnerabilities
    - 2 High Vulnerabilities
    - 4 Moderate Vulnerabilities

... Continued

## Other items since last Patch Tuesday



- Mozilla SeaMonkey 2.0.6 – 7/20/2010
  - Security release fixing 11 issues
    - 7 Critical software vulnerabilities
    - 1 Moderate software vulnerability
    - 3 Low software vulnerabilities
- Mozilla Thunderbird 3.1.1 - 7/20/2010
  - Security release fixing 10 issues
    - 5 Critical software vulnerabilities
    - 2 Moderate software vulnerabilities
    - 3 Low software vulnerabilities
- Mozilla Thunderbird 3.0.6 – 7/20/2010
  - Security release fixing 7 issues
    - 4 Critical software vulnerabilities
    - 1 Moderate software vulnerability
    - 2 Low software vulnerabilities

... Continued

## Other items since last Patch Tuesday



- Mozilla Firefox 3.6.8 – 7/23/2010
  - Security release fixing 1 issues
    - 1 Critical software vulnerability
- Opera 10.60 - 7/1/2010
  - Maintenance release
- Apple Safari 5.0.1 – 7/28/2010
  - Security release fixing 15 issues
    - 4 Critical software vulnerabilities
    - 1 Moderate software vulnerability
    - 2 Low software vulnerabilities

## Outstanding Vulnerabilities and Advisories



- ~~Microsoft Security Advisory 977377 (February 10, 2010)~~ **Expired with MS10-049**
  - Vulnerability in TLS/SSL Could Allow Spoofing

For audio, please call 1 (888) 268-4178 code: 94883955

## Contact Information:



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

For audio, please call 1 (888) 268-4178 code: 94883955