

# Microsoft Updates 2012

---

Microsoft Updates for Audiolog,  
Audiolog Interaction Quality (AIQ),  
Audiolog Interaction Review (AIR),  
and  
Insight Center (IC)

Microsoft Updates

April 2012

This document contains proprietary and confidential information of Verint Systems Inc. and may not be distributed to any persons or organizations for whom it was not intended.

© 2012 Verint Systems Inc. All Rights Reserved Worldwide.

Confidential and Proprietary Information of Verint Systems Inc.

All materials (regardless of form and including, without limitation, software applications, documentation, and any other information relating to Verint Systems, its products or services) are the exclusive property of Verint Systems Inc. Only expressly authorized individuals under obligations of confidentiality are permitted to review materials in this document. By reviewing these materials, you agree to not disclose these materials to any third party unless expressly authorized by Verint Systems, and to protect the materials as confidential and trade secret information. Any unauthorized review, retransmission, dissemination or other use of these materials is strictly prohibited. If you are not authorized to review these materials, please return these materials (and any copies) from where they were obtained. All materials found herein are provided "AS IS" and without warranty of any kind.

The Verint Systems Inc. products are protected by one or more of the following U.S., European or International Patents: USPN 5,659,768; USPN 5,790,798; USPN 6,278,978; USPN 6,370,574; USPN 6,404,857; USPN 6,510,220; USPN 6,757,361; USPN 6,782,093; USPN 6,952,732; USPN 6,959,405; USPN 7,047,296; USPN 7,149,788; USPN 7,155,399; USPN 7,203,285; USPN 6,959,078; USPN 6,724,887; USPN 7,216,162; European Patent 0 833 489; GB 2374249; and other provisional rights from one or more of the following Published US Patent Applications: US 10/061,469; US 10/061,489; US 10/061,491; US 11/388,854; US 11/388,944; US 11/389,471; US 10/818,787; US 11/166,630; US 11/129,811; US 11/477,124; US 11/509,553; US 11/509,550; US 11/509,554; US 11/509,552; US 11/509,549; US 11/509,551; US 11/583,381; US 10/181,103; US 09/825,589; US 09/899,895; US 11/037,604; US 11/237,456; US 09/680,131; US 11/359,356; US 11/359,319; US 11/359,532; US 11/359,359; US 11/359,358; US 11/359,357; US 11/359,195; US 11/385,499; US 11/394,496; US 11/393,286; US 11/396,061; US 11/395,992; US 11/394,410; US 11/394,794; US 11/395,350; US 11/395,759; US 60/799,228; US 11/479,926; US 11/479,841; US 11/479,925; US 11/479,056; US 11/478,714; US 11/479,899; US 11/479,506; US 11/479,267; US 60/837,816; US 11/528,267; US 11/529,132; US 11/540,281; US 11/540,322; US 11/529,947; US 11/540,902; US 11/541,056; US 11/529,942; US 11/540,282; US 11/529,946; US 11/540,320; US 11/529,842; US 11/540,904; US 11/541,252; US 11/541,313; US 11/540,086; US 11/540,739; US 11/540,185; US 11/540,107; US 11/540,900; US 10/610,780; US 10/832,509; US 11/608,340; US 11/608,350; US 11/608,358; US 10/771,315; US 10/771,409. Other U.S. and International Patents Pending.

VERINT, the VERINT logo, ACTIONABLE INTELLIGENCE, POWERING ACTIONABLE INTELLIGENCE, STAR-GATE, RELIANT, VANTAGE, X-TRACT, NEXTIVA, ULTRA, AUDIOLOG, WITNESS, the WITNESS logo, IMPACT 360, the IMPACT 360 logo, IMPROVE EVERYTHING, EQUALITY, CONTACTSTORE, and CLICK2STAFF are trademarks or registered trademarks of Verint Systems Inc. or its subsidiaries. Other trademarks mentioned are the property of their respective owners.

# Table of Contents

<a href="#">Introduction.....</a>	<a href="#">1</a>
<a href="#">Scope.....</a>	<a href="#">1</a>
<a href="#">April 2012.....</a>	<a href="#">1</a>
<a href="#">April 2012 Critical Updates.....</a>	<a href="#">2</a>
<a href="#">March 2012.....</a>	<a href="#">2</a>
<a href="#">March 2012 Critical Updates.....</a>	<a href="#">2</a>
<a href="#">March 2012 Important Updates.....</a>	<a href="#">2</a>
<a href="#">February 2012.....</a>	<a href="#">3</a>
<a href="#">February 2012 Critical Updates.....</a>	<a href="#">3</a>
<a href="#">February 2012 Important Updates.....</a>	<a href="#">3</a>
<a href="#">January 2012.....</a>	<a href="#">4</a>
<a href="#">January 2012 Critical Updates.....</a>	<a href="#">4</a>
<a href="#">January 2012 Important Updates.....</a>	<a href="#">4</a>
<a href="#">December 2011.....</a>	<a href="#">5</a>
<a href="#">December 2011 Critical Updates.....</a>	<a href="#">5</a>
<a href="#">December 2011 Important Updates.....</a>	<a href="#">6</a>
<a href="#">November 2011.....</a>	<a href="#">6</a>
<a href="#">November 2011 Critical Updates.....</a>	<a href="#">6</a>
<a href="#">November 2011 Important Updates.....</a>	<a href="#">7</a>
<a href="#">October 2011.....</a>	<a href="#">7</a>
<a href="#">October 2011 Critical Updates.....</a>	<a href="#">7</a>
<a href="#">October 2011 Important Updates.....</a>	<a href="#">7</a>
<a href="#">September 2011.....</a>	<a href="#">8</a>
<a href="#">September 2011 Important Updates.....</a>	<a href="#">8</a>
<a href="#">August 2011.....</a>	<a href="#">8</a>
<a href="#">August 2011 Critical Updates.....</a>	<a href="#">9</a>

August 2011 Important Updates.....	9
July 2011.....	10
July 2011 Important Updates.....	10
June 2011.....	10
June 2011 Critical Updates.....	11
June 2011 Important Updates.....	11
May 2011.....	12
April 2011.....	12
April 2011 Critical Updates.....	12
April 2011 Important Updates.....	13
March 2011.....	14
March 2011 Critical Updates.....	14
March 2011 Important Updates.....	14
February 2011.....	14
February 2011 Critical Updates.....	15
February 2011 Important Updates.....	15
January 2011.....	16
January 2011 Critical Updates.....	16
December 2010.....	16
December 2010 Critical Updates.....	16
December 2010 Important Updates.....	17
November 2010.....	17
October 2010.....	18
October 2010 Critical Updates.....	18
October 2010 Important Updates.....	18
September 2010.....	19
September 2010 Critical Updates.....	19
September 2010 Important Updates.....	20
August 2010.....	20

<a href="#">August 2010 Critical Updates.....</a>	<a href="#">21</a>
<a href="#">August 2010 Important Updates.....</a>	<a href="#">21</a>
<a href="#">July 2010.....</a>	<a href="#">22</a>
<a href="#">    July 2010 Critical Updates.....</a>	<a href="#">22</a>
<a href="#">June 2010.....</a>	<a href="#">22</a>
<a href="#">    June 2010 Critical Updates.....</a>	<a href="#">23</a>
<a href="#">    June 2010 Important Updates.....</a>	<a href="#">23</a>
<a href="#">May 2010.....</a>	<a href="#">24</a>
<a href="#">    May 2010 Critical Updates.....</a>	<a href="#">24</a>
<a href="#">April 2010.....</a>	<a href="#">24</a>
<a href="#">    April 2010 Critical Updates.....</a>	<a href="#">24</a>
<a href="#">    April 2010 Important Updates.....</a>	<a href="#">25</a>
<a href="#">March 2010.....</a>	<a href="#">25</a>
<a href="#">    March 2010 Important Updates.....</a>	<a href="#">25</a>
<a href="#">February 2010.....</a>	<a href="#">25</a>
<a href="#">    February 2010 Critical Updates.....</a>	<a href="#">26</a>
<a href="#">    February 2010 Important Updates.....</a>	<a href="#">26</a>
<a href="#">January 2010.....</a>	<a href="#">26</a>
<a href="#">    January 2010 Critical Updates.....</a>	<a href="#">27</a>
<a href="#">December 2009.....</a>	<a href="#">27</a>
<a href="#">    December 2009 Critical Updates.....</a>	<a href="#">27</a>
<a href="#">    December 2009 Important Updates.....</a>	<a href="#">27</a>
<a href="#">November 2009.....</a>	<a href="#">28</a>
<a href="#">    November 2009 Critical Updates.....</a>	<a href="#">28</a>
<a href="#">October 2009.....</a>	<a href="#">28</a>
<a href="#">    October 2009 Critical Updates.....</a>	<a href="#">28</a>
<a href="#">September 2009.....</a>	<a href="#">29</a>
<a href="#">    September 2009 Critical Updates.....</a>	<a href="#">29</a>
<a href="#">August 2009.....</a>	<a href="#">29</a>

August 2009 Critical Updates.....	30
August 2009 Important Updates.....	30
July 2009.....	30
July 2009 Critical Updates.....	30
June 2009.....	31
June 2009 Critical Updates.....	31
June 2009 Important Updates.....	31
May 2009.....	32
April 2009.....	32
April 2009 Critical Updates.....	32
April 2009 Moderate Updates.....	32
March 2009.....	33
March 2009 Critical Updates.....	34
March 2009 Important Updates.....	34
February 2009.....	34
February 2009 Critical Updates.....	34
January 2009.....	34
January 2009 Critical Updates.....	35

## Introduction

The document compiles the Microsoft Security Updates tested and certified for the Audiolog Suite of products. This document is updated on the third Tuesday of every month to include the latest Security Bulletins released by Microsoft.

This document contains the list of Microsoft Updates that are certified for Audiolog, Audiolog Interaction Quality (AIQ), Audiolog Interaction Review (AIR), and Audiolog Insight Center (IC) starting January 2009. For Updates released prior to this date, please contact Audiolog Technical Support.

## Scope

- Microsoft Security Bulletins are certified for the Service Pack level that is published on the Extranet as of the date of the release of the bulletin.
- Microsoft Security Bulletins are certified for Windows 2003 SP2, Windows XP SP3, Windows 2008 (Audiolog) and for Vista and Windows 7 (Audiolog Client).
- Microsoft Security Bulletins that are Critical, Moderate, and Important in risk levels are certified.
- Only Microsoft Security Updates that are applicable to the Audiolog suite of products are verified. Security Updates that are related to Microsoft products that are not installed on Audiolog Servers are not certified.
- Only Security Bulletins are certified as part of Microsoft Updates Releases. Hot fixes released for SQL Server, are not tested as part of this. Third party updates are rolled into Service Pack Releases for Audiolog.

## April 2012

### Tested Environments:

The Audiolog suite of products is certified for the following environments for April 2012. Please click on the links to learn more about the update.

### **Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 3, AIQ 4.1 SP4 Rollup 3, AIR 4.1 SP4 Rollup 3
- Audiolog Server 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

### **Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 3, Audiolog Client 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

## April 2012 Critical Updates

Microsoft Security Bulletin MS12-023

**Cumulative Security Update for Internet Explorer (2675157)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-023>

Microsoft Security Bulletin MS12-024

**Vulnerability in Windows Could Allow Remote Code Execution (2653956)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-024>

Microsoft Security Bulletin MS12-025

**Vulnerability in .NET Framework Could Allow Remote Code Execution (2671605)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-025>

## March 2012

### Tested Environments:

The Audiolog suite of products is certified for the following environments for March 2012. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

## March 2012 Critical Updates

Microsoft Security Bulletin MS12-020

**Vulnerabilities in Remote Desktop Could Allow Remote Code Execution (2671387)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-020>

## March 2012 Important Updates

Microsoft Security Bulletin MS12-018

**Vulnerability in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2641653)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-018>

## February 2012

### Tested Environments:

The Audiolog suite of products is certified for the following environments for February 2012. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

### Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

## February 2012 Critical Updates

Microsoft Security Bulletin MS12-008

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2660465)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-008>

Microsoft Security Bulletin MS12-010

**Cumulative Security Update for Internet Explorer (2647516)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-010>

Microsoft Security Bulletin MS12-013

**Vulnerability in C Run-Time Library Could Allow Remote Code Execution (2654428)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-013>

Microsoft Security Bulletin MS12-016

**Vulnerabilities in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2651026)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-016>

## February 2012 Important Updates

Microsoft Security Bulletin MS12-009

**Vulnerabilities in Ancillary Function Driver Could Allow Elevation of Privilege (2645640)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-009>

Microsoft Security Bulletin MS12-012

**Vulnerability in Color Control Panel Could Allow Remote Code Execution (2643719)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-012>

Microsoft Security Bulletin MS12-014

**Vulnerability in Indeo Codec Could Allow Remote Code Execution (2661637)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-014>

## January 2012

### Tested Environments:

The Audiolog suite of products is certified for the following environments for January 2012. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR5, AIQ 5 HFR5, AIR 5 HFR5, IC 5 HFR5

## January 2012 Critical Updates

Microsoft Security Bulletin MS12-004

**Vulnerabilities in Windows Media Could Allow Remote Code Execution (2639391)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-004>

## January 2012 Important Updates

Microsoft Security Bulletin MS12-001

**Vulnerability in Windows Kernel Could Allow Security Feature Bypass (2644615)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-001>

Microsoft Security Bulletin MS12-002

**Vulnerability in Windows Object Packager Could Allow Remote Code Execution (2603381)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-002>

Microsoft Security Bulletin MS12-003

**Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2646524)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-003>

Microsoft Security Bulletin MS12-005

**Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2584146)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-005>

Microsoft Security Bulletin MS12-006

**Vulnerability in SSL/TLS Could Allow Information Disclosure (2643584)**

<http://technet.microsoft.com/en-us/security/bulletin/ms12-006>

## December 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for December 2011. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR4, AIQ 5 HFR4, AIR 5 HFR4, IC 5 HFR4

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR4, AIQ 5 HFR4, AIR 5 HFR4, IC 5 HFR4

## December 2011 Critical Updates

Microsoft Security Bulletin MS11-087

**Vulnerability in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2639417)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-087>

Microsoft Security Bulletin MS11-090

**Cumulative Security Update of ActiveX Kill Bits (2618451)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-090>

Microsoft Security Bulletin MS11-092

**Vulnerability in Windows Media Could Allow Remote Code Execution (2648048)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-092>

Microsoft Security Bulletin MS11-100

**Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (2638420)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-100>

## December 2011 Important Updates

Microsoft Security Bulletin MS11-093

**Vulnerability in OLE Could Allow Remote Code Execution (2624667)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-093>

Microsoft Security Bulletin MS11-097

**Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2620712)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-097>

Microsoft Security Bulletin MS11-098

**Vulnerability in Windows Kernel Could Allow Elevation of Privilege (2633171)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-098>

Microsoft Security Bulletin MS11-099

**Cumulative Security Update for Internet Explorer (2618444)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-099>

## November 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for November 2011. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR4, AIQ 5 HFR4, AIR 5 HFR4, IC 5 HFR4

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR4, AIQ 5 HFR4, AIR 5 HFR4, IC 5 HFR4

## November 2011 Critical Updates

Microsoft Security Bulletin MS11-083

**Vulnerability in TCP/IP Could Allow Remote Code Execution (2588516)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-083>

## November 2011 Important Updates

Microsoft Security Bulletin MS11-085

**Vulnerability in Windows Mail and Windows Meeting Space Could Allow Remote Code Execution (2620704)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-085>

## October 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for October 2011. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR3, AIQ 5 HFR3, AIR 5 HFR3, IC 5 HFR3

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR3, AIQ 5 HFR3, AIR 5 HFR3, IC 5 HFR3

## October 2011 Critical Updates

Microsoft Security Bulletin MS11-078

**Vulnerability in .NET Framework and Microsoft Silverlight Could Allow Remote Code Execution (2604930)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-078>

Microsoft Security Bulletin MS11-081

**Cumulative Security Update for Internet Explorer (2586448)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-081>

## October 2011 Important Updates

Microsoft Security Bulletin MS11-075

**Vulnerability in Microsoft Active Accessibility Could Allow Remote Code Execution (2623699)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-075>

Microsoft Security Bulletin MS11-077

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (2567053)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-077>

Microsoft Security Bulletin MS11-080

**Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2592799)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-080>

## September 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for September 2011. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR3, AIQ 5 HFR3, AIR 5 HFR3, IC 5 HFR3

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR3, AIQ 5 HFR3, AIR 5 HFR3, IC 5 HFR3

## September 2011 Important Updates

Microsoft Security Bulletin MS11-071

**Vulnerability in Windows Components Could Allow Remote Code Execution (2570947)**

<http://technet.microsoft.com/en-us/security/bulletin/ms11-071>

## August 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for August 2011. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR3, AIQ 5 HFR3, AIR 5 HFR3, IC 5 HFR3

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR3, AIQ 5 HFR3, AIR 5 HFR3, IC 5 HFR3

## August 2011 Critical Updates

Microsoft Security Bulletin MS11-057

**Cumulative Security Update for Internet Explorer (2559049)**

<http://www.microsoft.com/technet/security/bulletin/MS11-057.msp>

## August 2011 Important Updates

Microsoft Security Bulletin MS11-059

**Vulnerability in Data Access Components Could Allow Remote Code Execution (2560656)**

<http://www.microsoft.com/technet/security/bulletin/ms11-059.msp>

Microsoft Security Bulletin MS11-061

**Vulnerability in Remote Desktop Web Access Could Allow Elevation of Privilege (2546250)**

<http://www.microsoft.com/technet/security/bulletin/ms11-061.msp>

Microsoft Security Bulletin MS11-062

**Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege (2566454)**

<http://www.microsoft.com/technet/security/bulletin/ms11-062.msp>

Microsoft Security Bulletin MS11-063

**Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2567680)**

<http://www.microsoft.com/technet/security/bulletin/ms11-063.msp>

Microsoft Security Bulletin MS11-064

**Vulnerabilities in TCP/IP Stack Could Allow Denial of Service (2563894)**

<http://www.microsoft.com/technet/security/bulletin/ms11-064.msp>

Microsoft Security Bulletin MS11-065

**Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (2570222)**

<http://www.microsoft.com/technet/security/bulletin/ms11-065.mspx>

Microsoft Security Bulletin MS11-066

**Vulnerability in Microsoft Chart Control Could Allow Information Disclosure (2567943)**

<http://www.microsoft.com/technet/security/bulletin/ms11-066.mspx>

Microsoft Security Bulletin MS11-067

**Vulnerability in Microsoft Report Viewer Could Allow Information Disclosure (2578230)**

<http://www.microsoft.com/technet/security/bulletin/ms11-067.mspx>

## July 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for July 2011. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5 HFR2, AIQ 5 HFR2, AIR 5 HFR2, IC 5 HFR2

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 HFR2, AIQ 5 HFR2, AIR 5 HFR2, IC 5 HFR2

## July 2011 Important Updates

Microsoft Security Bulletin MS11-054

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2555917)**

<http://www.microsoft.com/technet/security/bulletin/ms11-054.mspx>

Microsoft Security Bulletin MS11-056

**Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2507938)**

<http://www.microsoft.com/technet/security/bulletin/ms11-056.mspx>

## June 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for June 2011. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 (only upgrades) and Windows XP Professional, SP3 and Windows 2008:**

- Audiolog Server 4 SP4 Rollup 2, AIQ 4.1 SP4 Rollup 2, AIR 4.1 SP4 Rollup 2
- Audiolog Server 5GA, AIQ 5 GA, AIR 5 GA

**Vista SP2, Windows XP Professional, Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 2, Audiolog Client 5 GA

## June 2011 Critical Updates

Microsoft Security Bulletin MS11-038

**Vulnerability in OLE Automation Could Allow Remote Code Execution (2476490)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-038.mspx>

Microsoft Security Bulletin MS11-042

**Vulnerabilities in Distributed File System Could Allow Remote Code Execution (2535512)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-042.mspx>

Microsoft Security Bulletin MS11-043

**Vulnerability in SMB Client Could Allow Remote Code Execution (2536276)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-043.mspx>

Microsoft Security Bulletin MS11-044

**Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-044.mspx>

Microsoft Security Bulletin MS11-050

**Cumulative Security Update for Internet Explorer (2530548)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-050.mspx>

Microsoft Security Bulletin MS11-052

**Vulnerability in Vector Markup Language Could Allow Remote Code Execution (2544521)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-052.mspx>

## June 2011 Important Updates

Microsoft Security Bulletin MS11-037

**Vulnerability in MHTML Could Allow Information Disclosure (2544893)**

<http://www.microsoft.com/technet/security/bulletin/ms11-037.msp>

Microsoft Security Bulletin MS11-046

**Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege (2503665)**

<http://www.microsoft.com/technet/security/bulletin/MS11-046.msp>

## May 2011

There are no critical or important updates relevant to Audiolog, AIR, and AIQ for the month of May.

## April 2011

### Tested Environments:

The Audiolog suite of products is certified for the following environments for April 2011. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ 2.0

### Windows 2003 Professional, SP2 and Windows XP Professional, SP3 and Vista:

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4
- Audiolog Server and Client 5 GA, AIQ 5 GA, AIR 5 GA

### Windows 7 32 and 64 bit:

- Audiolog Client 4 SP4 Rollup 1

## April 2011 Critical Updates

Microsoft Security Bulletin MS11-018

**Cumulative Security Update for Internet Explorer (2497640)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-018.msp>

Microsoft Security Bulletin MS11-019

**Vulnerabilities in SMB Client Could Allow Remote Code Execution (2511455)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-019.msp>

Microsoft Security Bulletin MS11-020

**Vulnerability in SMB Server Could Allow Remote Code Execution (2508429)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-020.msp>

Microsoft Security Bulletin MS11-027

**Cumulative Security Update of ActiveX Kill Bits (2508272)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-027.msp>

Microsoft Security Bulletin MS11-028

**Vulnerability in .NET Framework Could Allow Remote Code Execution (2484015)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-028.msp>

Microsoft Security Bulletin MS11-029

**Vulnerability in GDI+ Could Allow Remote Code Execution (2489979)**

<http://www.microsoft.com/technet/security/bulletin/MS11-029.msp>

Microsoft Security Bulletin MS11-030

**Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553)**

<http://www.microsoft.com/technet/security/bulletin/ms11-030.msp>

Microsoft Security Bulletin MS11-032

**Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2507618)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-032.msp>

## **April 2011 Important Updates**

Microsoft Security Bulletin MS11-024

**Vulnerability in Windows Fax Cover Page Editor Could Allow Remote Code Execution (2527308)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-024.msp>

Microsoft Security Bulletin MS11-026

**Vulnerability in MHTML Could Allow Information Disclosure (2503658)**

<http://www.microsoft.com/technet/security/bulletin/ms11-026.msp>

Microsoft Security Bulletin MS11-033

**Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2485663)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-033.msp>

Microsoft Security Bulletin MS11-034

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2506223)**

<http://www.microsoft.com/technet/security/bulletin/ms11-034.msp>

## March 2011

### **Tested Environments:**

The Audiolog suite of products is certified for the following environments for March 2011. Please click on the links to learn more about the update.

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ 2.0

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3 and Vista:**

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4
- Audiolog Server and Client 5 GA, AIQ 5 GA, AIR 5 GA

### **Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 1

## March 2011 Critical Updates

Microsoft Security Bulletin MS11-015

### **Vulnerabilities in Windows Media Could Allow Remote Code Execution (2510030)**

<http://www.microsoft.com/technet/security/bulletin/ms11-015.mspx>

## March 2011 Important Updates

Microsoft Security Bulletin MS11-017

### **Vulnerability in Remote Desktop Client Could Allow Remote Code Execution (2508062)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-017.mspx>

## February 2011

### **Tested Environments:**

The Audiolog suite of products is certified for the following environments for February 2011. Please click on the links to learn more about the update.

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ 2.0

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3 and Vista:**

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4
- Audiolog Server and Client 5 GA, AIQ 5 GA, AIR 5 GA

### **Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 1

## February 2011 Critical Updates

Microsoft Security Bulletin MS11-003

**Cumulative Security Update for Internet Explorer (2482017)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-003.msp>

Microsoft Security Bulletin MS11-006

**Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution (2483185)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-006.msp>

Microsoft Security Bulletin MS11-007

**Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution (2485376)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-007.msp>

## February 2011 Important Updates

Microsoft Security Bulletin MS11-009

**Vulnerability in JScript and VBScript Scripting Engines Could Allow Information Disclosure (2475792)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-009.msp>

Microsoft Security Bulletin MS11-010

**Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (2476687)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-010.msp>

Microsoft Security Bulletin MS11-011

**Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (2393802)**

<http://www.microsoft.com/technet/security/bulletin/ms11-011.msp>

Microsoft Security Bulletin MS11-012

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2479628)**

<http://www.microsoft.com/technet/security/bulletin/ms11-012.msp>

Microsoft Security Bulletin MS11-013

**Vulnerabilities in Kerberos Could Allow Elevation of Privilege (2496930)**

<http://www.microsoft.com/technet/security/bulletin/ms11-013.msp>

Microsoft Security Bulletin MS11-014

**Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege (2478960)**

<http://www.microsoft.com/technet/security/Bulletin/MS11-014.msp>

## January 2011

### **Tested Environments:**

The Audiolog suite of products is certified for the following environments for January 2011. Please click on the links to learn more about the update.

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ 2.0

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3 and Vista:**

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4

#### **Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 1

## January 2011 Critical Updates

Microsoft Security Bulletin MS11-002

**Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution (2451910)**

<http://www.microsoft.com/technet/security/bulletin/MS11-002.msp>

## December 2010

### **Tested Environments:**

The Audiolog suite of products is certified for the following environments for December 2010. Please click on the links to learn more about the update.

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ 2.0

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3 and Vista:**

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4

#### **Windows 7 32 and 64 bit:**

- Audiolog Client 4 SP4 Rollup 1

## December 2010 Critical Updates

Microsoft Security Bulletin MS10-090

**Cumulative Security Update for Internet Explorer (2416400)**

<http://www.microsoft.com/technet/security/bulletin/MS10-090.msp>

Microsoft Security Bulletin MS10-091

**Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (2296199)**

<http://www.microsoft.com/technet/security/bulletin/MS10-091.msp>

## December 2010 Important Updates

Microsoft Security Bulletin MS10-095

**Vulnerability in Microsoft Windows Could Allow Remote Code Execution (2385678)**

<http://www.microsoft.com/technet/security/bulletin/MS10-095.msp>

Microsoft Security Bulletin MS10-096

**Vulnerability in Windows Address Book Could Allow Remote Code Execution (2423089)**

<http://www.microsoft.com/technet/security/bulletin/MS10-096.msp>

Microsoft Security Bulletin MS10-097

**Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution (2443105)**

<http://www.microsoft.com/technet/security/bulletin/MS10-097.msp>

Microsoft Security Bulletin MS10-098

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2436673)**

<http://www.microsoft.com/technet/security/bulletin/ms10-098.msp>

Microsoft Security Bulletin MS10-099

**Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege (2440591)**

<http://www.microsoft.com/technet/security/bulletin/ms10-099.msp>

Microsoft Security Bulletin MS10-100

**Vulnerability in Consent User Interface Could Allow Elevation of Privilege (2442962)**

<http://www.microsoft.com/technet/security/bulletin/MS10-100.msp>

## November 2010

There are no critical or important updates relevant to Audiolog, AIR, and AIQ for the month of November.

## October 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for October 2010. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

### Windows 2003 Professional, SP2 and Windows XP Professional, SP3 and Vista:

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## October 2010 Critical Updates

Microsoft Security Bulletin MS10-071

### Cumulative Security Update for Internet Explorer (2360131)

<http://www.microsoft.com/technet/security/bulletin/ms10-071.mspx>

Microsoft Security Bulletin MS10-075

### Vulnerability in Media Player Network Sharing Service Could Allow Remote Code Execution (2281679)

<http://www.microsoft.com/technet/security/bulletin/MS10-075.mspx>

Microsoft Security Bulletin MS10-076

### Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)

<http://www.microsoft.com/technet/security/bulletin/MS10-076.mspx>

## October 2010 Important Updates

Microsoft Security Bulletin MS10-073

### Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (981957)

<http://www.microsoft.com/technet/security/bulletin/MS10-073.mspx>

Microsoft Security Bulletin MS10-078

### Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege (2279986)

<http://www.microsoft.com/technet/security/bulletin/MS10-078.mspx>

Microsoft Security Bulletin MS10-081

### Vulnerability in Windows Common Control Library Could Allow Remote Code Execution (2296011)

<http://www.microsoft.com/technet/security/bulletin/MS10-081.msp>

Microsoft Security Bulletin MS10-082

**Vulnerability in Windows Media Player Could Allow Remote Code Execution (2378111)**

<http://www.microsoft.com/technet/security/bulletin/MS10-082.msp>

Microsoft Security Bulletin MS10-083

**Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution (2405882)**

<http://www.microsoft.com/technet/security/bulletin/ms10-083.msp>

Microsoft Security Bulletin MS10-084

**Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege (2360937)**

<http://www.microsoft.com/technet/security/bulletin/MS10-084.msp>

Microsoft Security Bulletin MS10-085

**Vulnerability in SChannel Could Allow Denial of Service (2207566)**

<http://www.microsoft.com/technet/security/bulletin/MS10-085.msp>

## September 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for September 2010. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

### Windows 2003 Professional, SP2 and Windows XP Professional, SP3:

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## September 2010 Critical Updates

Microsoft Security Bulletin MS10-061

**Vulnerability in Print Spooler Service Could Allow Remote Code Execution (2347290)**

<http://www.microsoft.com/technet/security/bulletin/ms10-061.msp>

Microsoft Security Bulletin MS10-062

**Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (975558)**

<http://www.microsoft.com/technet/security/bulletin/MS10-062.msp>

Microsoft Security Bulletin MS10-063

**Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2320113)**

<http://www.microsoft.com/technet/security/bulletin/MS10-063.msp>

## September 2010 Important Updates

Microsoft Security Bulletin MS10-065

**Vulnerabilities in Microsoft Internet Information Services (IIS) Could Allow Remote Code Execution (2267960)**

<http://www.microsoft.com/technet/security/bulletin/MS10-065.msp>

Microsoft Security Bulletin MS10-066

**Vulnerability in Remote Procedure Call Could Allow Remote Code Execution (982802)**

<http://www.microsoft.com/technet/security/bulletin/ms10-066.msp>

Microsoft Security Bulletin MS10-067

**Vulnerability in WordPad Text Converters Could Allow Remote Code Execution (2259922)**

<http://www.microsoft.com/technet/security/bulletin/MS10-067.msp>

Microsoft Security Bulletin MS10-069

**Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege (2121546)**

<http://www.microsoft.com/technet/security/bulletin/MS10-069.msp>

## August 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for August 2010. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

### Windows 2003 Professional, SP2 and Windows XP Professional, SP3:

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4

## August 2010 Critical Updates

Microsoft Security Bulletin MS10-046

**Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)**

<http://www.microsoft.com/technet/security/bulletin/MS10-046.msp>

Microsoft Security Bulletin MS10-049

**Vulnerabilities in SChannel Could Allow Remote Code Execution (980436)**

<http://www.microsoft.com/technet/security/bulletin/MS10-049.msp>

Microsoft Security Bulletin MS10-051

**Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution (2079403)**

<http://www.microsoft.com/technet/security/bulletin/ms10-051.msp>

Microsoft Security Bulletin MS10-052

**Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (2115168)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-052.msp>

Microsoft Security Bulletin MS10-053

**Cumulative Security Update for Internet Explorer (2183461)**

<http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>

Microsoft Security Bulletin MS10-054

**Vulnerabilities in SMB Server Could Allow Remote Code Execution (982214)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-054.msp>

Microsoft Security Bulletin MS10-055

**Vulnerability in Cinepak Codec Could Allow Remote Code Execution (982665)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-055.msp>

Microsoft Security Bulletin MS10-060

**Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution (2265906)**

<http://www.microsoft.com/technet/security/bulletin/MS10-060.msp>

## August 2010 Important Updates

Microsoft Security Bulletin MS10-047

**Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (981852)**

<http://www.microsoft.com/technet/security/bulletin/MS10-047.msp>

Microsoft Security Bulletin MS10-048

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (2160329)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-048.msp>

Microsoft Security Bulletin MS10-050

**Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (981997)**

<http://www.microsoft.com/technet/security/bulletin/MS10-050.msp>

Microsoft Security Bulletin MS10-058

**Vulnerabilities in TCP/IP Could Allow Elevation of Privilege (978886)**

<http://www.microsoft.com/technet/security/bulletin/MS10-058.msp>

Microsoft Security Bulletin MS10-059

**Vulnerabilities in the Tracing Feature for Services Could Allow an Elevation of Privilege (982799)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-059.msp>

## July 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for July 2010. Please click on the links to learn more about the update.

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4

## July 2010 Critical Updates

Microsoft Security Bulletin MS10-042

**Vulnerabilities in Help and SupportCenter Could Allow Remote Code Execution (2229593)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-042.msp>

## June 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for June 2010. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP4, AIQ 4.1 SP4, AIR 4.1 SP4

## June 2010 Critical Updates

Microsoft Security Bulletin MS10-033

**Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)**

<http://www.microsoft.com/technet/security/bulletin/ms10-033.msp>

Microsoft Security Bulletin MS10-034

**Cumulative Security Update of ActiveX Kill Bits (980195)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-034.msp>

Microsoft Security Bulletin MS10-035

**Cumulative Security Update for Internet Explorer (982381)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-035.msp>

## June 2010 Important Updates

Microsoft Security Bulletin MS10-032

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (979559)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-032.msp>

Microsoft Security Bulletin MS10-037

**Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege (980218)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-037.msp>

Microsoft Security Bulletin MS10-040

**Vulnerability in Internet Information Services Could Allow Remote Code Execution (982666)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-040.msp>

## May 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for May 2010. Please click on the links to learn more about the update.

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## May 2010 Critical Updates

Microsoft Security Bulletin MS10-030

**Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)**

<http://www.microsoft.com/technet/security/bulletin/MS10-030.mspx>

## April 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for April 2010. Please click on the links to learn more about the update.

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

#### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## April 2010 Critical Updates

Microsoft Security Bulletin MS10-020

**Vulnerabilities in SMB Client Could Allow Remote Code Execution (980232)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-020.mspx>

Microsoft Security Bulletin MS10-026

**Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-026.msp>

Microsoft Security Bulletin MS10-027

**Vulnerability in Windows Media Player Could Allow Remote Code Execution (979402)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-027.msp>

## April 2010 Important Updates

Microsoft Security Bulletin MS10-021

**Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (979683)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-021.msp>

Microsoft Security Bulletin MS10-022

**Vulnerability in VBScript Could Allow Remote Code Execution (981169)**

<http://www.microsoft.com/technet/security/bulletin/MS10-022.msp>

## March 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for March 2010. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

### Windows 2003 Professional, SP2 and Windows XP Professional, SP3:

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## March 2010 Important Updates

Microsoft Security Bulletin MS10-016

**Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)**

<http://www.microsoft.com/technet/security/bulletin/ms10-016.msp>

## February 2010

### Tested Environments:

The Audiolog suite of products is certified for the following environments for February 2010. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## February 2010 Critical Updates

Microsoft Security Bulletin MS10-006

**Vulnerabilities in SMB Client Could Allow Remote Code Execution (978251)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-006.aspx>

Microsoft Security Bulletin MS10-007

**Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (975713)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-007.aspx>

Microsoft Security Bulletin MS10-008

**Cumulative Security Update of ActiveX Kill Bits (978262)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-008.aspx>

## February 2010 Important Updates

Microsoft Security Bulletin MS10-011

**Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege (978037)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-011.aspx>

Microsoft Security Bulletin MS10-012

**Vulnerabilities in SMB Server Could Allow Remote Code Execution (971468)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-012.aspx>

Microsoft Security Bulletin MS10-015

**Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (977165)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-015.aspx>

## January 2010

**Tested Environments:**

The Audiolog suite of products is certified for the following environments for January 2010. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## January 2010 Critical Updates

Microsoft Security Bulletin MS10-001

**Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)**

<http://www.microsoft.com/technet/security/Bulletin/MS10-001.msp>

## December 2009

**Tested Environments:**

The Audiolog suite of products is certified for the following environments for December 2009. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## December 2009 Critical Updates

Microsoft Security Bulletin MS09-071

**Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution (974318)**

<http://www.microsoft.com/technet/security/bulletin/MS09-071.msp>

Microsoft Security Bulletin MS09-072

**Cumulative Security Update for Internet Explorer (976325)**

<http://www.microsoft.com/technet/security/bulletin/ms09-072.msp>

## December 2009 Important Updates

Microsoft Security Bulletin MS09-069

**Authority Subsystem Service Could Allow Denial of Service (974392)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-069.mspx>

## November 2009

**Tested Environments:**

The Audiolog suite of products is certified for the following environments for November 2009. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3 and SP4, AIQ 4.1 SP3 and SP4, AIR 4.1 SP3 and SP4

## November 2009 Critical Updates

Microsoft Security Bulletin MS09-065

**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution (969947)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-065.mspx>

## October 2009

**Tested Environments:**

The Audiolog suite of products is certified for the following environments for October 2009. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## October 2009 Critical Updates

Microsoft Security Bulletin MS09-052

**Vulnerability in Windows Media Player Could Allow Remote Code Execution (974112)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-052.mspx>

Microsoft Security Bulletin MS09-054

**Cumulative Security Update for Internet Explorer (974455)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-054.msp>

Microsoft Security Bulletin MS09-055

**Cumulative Security Update of ActiveX Kill Bits (973525)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-055.msp>

## September 2009

### Tested Environments:

The Audiolog suite of products is certified for the following environments for September 2009. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## September 2009 Critical Updates

Microsoft Security Bulletin MS09-045

**Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution (971961)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-045.msp>

Microsoft Security Bulletin MS09-048

**Vulnerabilities in Windows TCP/IP Could Allow Remote Code Execution (967723)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-048.msp>

Microsoft Security Bulletin MS09-046

**Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution (956844)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-046.msp>

## August 2009

### Tested Environments:

The Audiolog suite of products is certified for the following environments for August 2009. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## August 2009 Critical Updates

Microsoft Security Bulletin MS09-038

**Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution (971557)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-038.msp>

## August 2009 Important Updates

Microsoft Security Bulletin MS09-041

**Vulnerability in Workstation Service Could Allow Elevation of Privilege (971657)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-041.msp>

Microsoft Security Bulletin MS09-040

**Vulnerability in Message Queuing Could Allow Elevation of Privilege (971032)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-040.msp>

Microsoft Security Bulletin MS09-042

**Vulnerability in Telnet Could Allow Remote Code Execution (960859)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-042.msp>

## July 2009

### Tested Environments:

The Audiolog suite of products is certified for the following environments for June 2009. Please click on the links to learn more about the update.

**Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

**Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## July 2009 Critical Updates

Microsoft Security Bulletin MS09-028

**Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution (971633)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-028.msp>

Microsoft Security Bulletin MS09-029

**Vulnerabilities in the Embedded OpenType Font Engine Could Allow Remote Code Execution (961371)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-029.msp>

Microsoft Security Bulletin MS09-032

**Cumulative Security Update of ActiveX Kill Bits (973346)**

<http://www.microsoft.com/technet/security/bulletin/MS09-032.msp>

## June 2009

### Tested Environments:

The Audiolog suite of products is certified for the following environments for June 2009. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0

### Windows 2003 Professional, SP2 and Windows XP Professional, SP3:

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## June 2009 Critical Updates

Microsoft Security Bulletin MS09-022

**Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-022.msp>

Microsoft Security Bulletin MS09-019

**Cumulative Security Update for Internet Explorer (969897)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-019.msp>

## June 2009 Important Updates

Microsoft Security Bulletin MS09-026

**Vulnerability in RPC Could Allow Elevation of Privilege (970238)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-026.msp>

Microsoft Security Bulletin MS09-025

**Kernel Could Allow Elevation of Privilege (968537)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-025.msp>

Microsoft Security Bulletin MS09-020

**Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-020.mspx>

## May 2009

There are no critical, moderate, or important updates relevant to Audiolog, AIR, and AIQ for the month of May.

## April 2009

### Tested Environments:

The Audiolog suite of products is certified for the following environments for April 2009. Please click on the links to learn more about the update.

### Windows 2003 Professional, SP2 and Windows XP Professional, SP2:

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0
- Audiolog Server and Client 4 SP2, AIQ 4.1 SP2, AIR 4.1 SP2

### Windows 2003 Professional, SP2 and Windows XP Professional, SP3:

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## April 2009 Critical Updates

Microsoft Security Bulletin MS09-013

**Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)**

<http://www.microsoft.com/technet/security/bulletin/MS09-013.mspx>

Microsoft Security Bulletin MS09-011

**Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373)**

<http://www.microsoft.com/technet/security/Bulletin/ms09-011.mspx>

Microsoft Security Bulletin MS09-014

**Cumulative Security Update for Internet Explorer (963027)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-014.mspx>

## April 2009 Moderate Updates

Microsoft Security Bulletin MS09-015

**Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-015.msp>

## March 2009

### **Tested Environments:**

Audiolog Suite of products is certified for the following environments for March 2009. Please click on the links to learn more about the update.

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0
- Audiolog Server and Client 4 SP1, AIQ 4.1 SP1, AIR 4.1 SP1
- Audiolog Server and Client 4 SP2, AIQ 4.1 SP2, AIR 4.1 SP2

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## March 2009 Critical Updates

Microsoft Security Bulletin MS09-006

### **Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)**

<http://www.microsoft.com/technet/security/bulletin/MS09-006.msp>

## March 2009 Important Updates

Microsoft Security Bulletin MS09-007

### **Vulnerability in SChannel Could Allow Spoofing (960225)**

<http://www.microsoft.com/technet/security/bulletin/MS09-007.msp>

## February 2009

Audiolog is certified for the MS Update released in February 2009 for the following environments:

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0
- Audiolog Server and Client 4 SP1, AIQ 4.1 SP1, AIR 4.1 SP1
- Audiolog Server and Client 4 SP2, AIQ 4.1 SP2, AIR 4.1 SP2

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3

## February 2009 Critical Updates

Microsoft Security Bulletin MS09-002

### **Cumulative Security Update for Internet Explorer (961260)**

<http://www.microsoft.com/technet/security/Bulletin/MS09-002.msp>

## January 2009

Audiolog is certified for the MS Update released in January 2009 for the following environments:

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP2:**

- Audiolog 3.3, Client 3.3, MIR 3.3, AIQ2.0
- Audiolog Server and Client 4 SP1, AIQ 4.1 SP1, AIR 4.1 SP1 )
- Audiolog Server and Client 4 SP2, AIQ 4.1 SP2, AIR 4.1 SP2 )

### **Windows 2003 Professional, SP2 and Windows XP Professional, SP3:**

- Audiolog Server and Client 4 SP3, AIQ 4.1 SP3, AIR 4.1 SP3 )

## January 2009 Critical Updates

Microsoft Security Bulletin MS09-001

### **Vulnerabilities in SMB Could Allow Remote Code Execution (958687)**

<http://www.microsoft.com/technet/security/Bulletin/ms09-001.msp>

## Verint. Powering Actionable Intelligence.®

Verint® Systems Inc. is a leading global provider of analytic software-based solutions for enterprise optimization and security. Verint solutions help organizations make sense of the vast voice, video, and data available to them, transforming this information into *actionable intelligence* for better decisions and highly effective performance.

Since 1994, Verint has been committed to developing innovative solutions that help global organizations achieve their most important objectives. Today, organizations in over 100 countries use Verint solutions to enhance security, boost operational efficiency, and fuel profitability.