

**TANDBERG**

# Server Appliance

## Security Updates Release Notes

**Software Version**

**D50558 Revision 5**

**June 2009**

## TABLE OF CONTENTS

<b>SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES</b>	
<b>2009-6</b> .....	<b>4</b>
Introduction .....	4
<i>Security Updates Overview</i> .....	4
Microsoft Security Updates.....	4
<i>June 2009</i> .....	4
<i>May 2009</i> .....	5
<b>SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES</b>	
<b>2009-4</b> .....	<b>6</b>
Introduction .....	6
<i>Security Updates Overview</i> .....	6
Microsoft Security Updates.....	6
<i>April 2009</i> .....	6
<b>SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES</b>	
<b>2009-3</b> .....	<b>7</b>
Introduction .....	7
<i>Security Updates Overview</i> .....	7
Microsoft Security Updates.....	7
<i>March 2009</i> .....	7
<b>SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES</b>	
<b>2009-2</b> .....	<b>8</b>
Introduction .....	8
<i>Security Updates Overview</i> .....	8
Microsoft Security Updates.....	8
<i>February 2009</i> .....	8
<b>SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES</b>	
<b>2009-1</b> .....	<b>9</b>
Introduction .....	9
<i>Security Updates Overview</i> .....	9
Microsoft Security Updates.....	9
<i>January 2009</i> .....	9
<i>December 2008</i> .....	10
<i>November 2008</i> .....	10
<i>October 2008 – Out-of-Band Update</i> .....	10
<i>October 2008</i> .....	10
<i>September 2008</i> .....	10
<i>August 2008</i> .....	11
<i>July 2008</i> .....	11
Supplemental Notes .....	12
<i>Security Patches</i> .....	12
<i>References/Related Documents</i> .....	12
<i>Getting the Software</i> .....	12
<i>Installation of Security Patch</i> .....	13

## ***DOCUMENT REVISION HISTORY***

Revision 5	Included Release of Security Update 2009-6
Revision 4	Included Release of Security Update 2009-4
Revision 3	Included Release of Security Update 2009-3
Revision 2	Included Release of Security Update 2009-2
Revision 1	Initial Release of Security Update 2009-1

# SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES 2009-6

## Introduction

These release notes describe the features and capabilities included in the TANDBERG Server Appliance Security Updates software version 2009-6 released on 18 June 2009.

## Security Updates Overview

This version of the Security Updates 2009-6 installs the following Microsoft Security Updates.

This Installer includes Microsoft security updates for TANDBERG Server Appliances with Windows Server 2003 Service Pack 2 installed. Please ensure that the Windows Server Service Pack 2 is installed on the server before proceeding with this installation.

Visit [http://www.tandberg.com/support/tandberg\\_device\\_security.jsp](http://www.tandberg.com/support/tandberg_device_security.jsp) for instructions on how to install Microsoft Windows Service Pack 2 on the TANDBERG Server Appliance.

**Note:** If no updates have been applied to the server since 2008, the program list within 'Add/Remove Programs' will now display both 'TANDBERG Content Server Updates' as well as 'TANDBERG Server Appliance Security Updates' after this update is applied. This is due to the name change with the security updates and can be safely ignored.

This update contains updates released from July 2008, for updates prior to this please install 'TSA Security Updates 2008-6'.

**IMPORTANT:** The only supported installation methods is through either the local box (e.g. USB keyboard and monitor locally connected) or through the Microsoft Remote Desktop Utility installed locally on a remote PC. Other utilities, including web-based Remote Desktop Utilities are not supported and should not be used under any circumstances.

## Microsoft Security Updates

### June 2009

The following security updates were released by Microsoft in April 2009 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 961501	<a href="#">Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution (961501)</a>
KB 969897	<a href="#">Cumulative Security Update for Internet Explorer (969897)</a>
KB 970238	<a href="#">Vulnerability in RPC Could Allow Elevation of Privilege (970238)</a>
KB 968537	<a href="#">Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (968537)</a>
KB 970483	<a href="#">Vulnerabilities in Internet Information Services (IIS) Could Allow Elevation of Privilege (970483)</a>

**May 2009**

There were no updates released in May 2009 that apply to the TANDBERG Server Appliance or any related services on the Server Appliance.

# SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES 2009-4

## Introduction

These release notes describe the features and capabilities included in the TANDBERG Server Appliance Security Updates software version 2009-4 released on 22 April 2009.

## Security Updates Overview

This version of the Security Updates 2009-4 installs the following Microsoft Security Updates.

This Installer includes Microsoft security updates for TANDBERG Server Appliances with Windows Server 2003 Service Pack 2 installed. Please ensure that the Windows Server Service Pack 2 is installed on the server before proceeding with this installation.

Visit [http://www.tandberg.com/support/tandberg\\_device\\_security.jsp](http://www.tandberg.com/support/tandberg_device_security.jsp) for instructions on how to install Microsoft Windows Service Pack 2 on the TANDBERG Server Appliance.

**Note:** If no updates have been applied to the server since 2008, the program list within 'Add/Remove Programs' will now display both 'TANDBERG Content Server Updates' as well as 'TANDBERG Server Appliance Security Updates' after this update is applied. This is due to the name change with the security updates and can be safely ignored.

This update contains updates released from July 2008, for updates prior to this please install 'TSA Security Updates 2008-6'.

**IMPORTANT:** The only supported installation methods is through either the local box (e.g. USB keyboard and monitor locally connected) or through the Microsoft Remote Desktop Utility installed locally on a remote PC. Other utilities, including web-based Remote Desktop Utilities are not supported and should not be used under any circumstances.

## Microsoft Security Updates

### April 2009

The following security updates were released by Microsoft in April 2009 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 959426	<a href="#">Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege (959426)</a>
KB 959454	<a href="#">Vulnerabilities in Windows Could Allow Elevation of Privilege (959454)</a>
KB 963027	<a href="#">Cumulative Security Update for Internet Explorer (963027)</a>
KB 961373	<a href="#">Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (961373)</a>
KB 960803	<a href="#">Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution (960803)</a>

# SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES 2009-3

## Introduction

These release notes describe the features and capabilities included in the TANDBERG Server Appliance Security Updates software version 2009-3 released on 17 March 2009.

## Security Updates Overview

This version of the Security Updates 2009-3 installs the following Microsoft Security Updates.

This Installer includes Microsoft security updates for TANDBERG Server Appliances with Windows Server 2003 Service Pack 2 installed. Please ensure that the Windows Server Service Pack 2 is installed on the server before proceeding with this installation.

Visit [http://www.tandberg.com/support/tandberg\\_device\\_security.jsp](http://www.tandberg.com/support/tandberg_device_security.jsp) for instructions on how to install Microsoft Windows Service Pack 2 on the TANDBERG Server Appliance.

**Note:** If no updates have been applied to the server since 2008, the program list within 'Add/Remove Programs' will now display both 'TANDBERG Content Server Updates' as well as 'TANDBERG Server Appliance Security Updates' after this update is applied. This is due to the name change with the security updates and can be safely ignored.

This update contains updates released from July 2008, for updates prior to this please install 'TSA Security Updates 2008-6'.

**IMPORTANT:** The only supported installation methods is through either the local box (e.g. USB keyboard and monitor locally connected) or through the Microsoft Remote Desktop Utility installed locally on a remote PC. Other utilities, including web-based Remote Desktop Utilities are not supported and should not be used under any circumstances.

## Microsoft Security Updates

### March 2009

The following security updates were released by Microsoft in March 2009 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 960225	<a href="#">Vulnerability in SChannel Could Allow Spoofing (960225)</a>
KB 958690	<a href="#">Vulnerabilities in Windows Kernel Could Allow Remote Code Execution (958690)</a>

# SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES 2009-2

## Introduction

These release notes describe the features and capabilities included in the TANDBERG Server Appliance Security Updates software version 2009-2 released on 17 February 2009.

## Security Updates Overview

This version of the Security Updates 2009-2 installs the following Microsoft Security Updates.

This Installer includes Microsoft security updates for TANDBERG Server Appliances with Windows Server 2003 Service Pack 2 installed. Please ensure that the Windows Server Service Pack 2 is installed on the server before proceeding with this installation.

Visit [http://www.tandberg.com/support/tandberg\\_device\\_security.jsp](http://www.tandberg.com/support/tandberg_device_security.jsp) for instructions on how to install Microsoft Windows Service Pack 2 on the TANDBERG Server Appliance.

**Note:** If no updates have been applied to the server since 2008, the program list within 'Add/Remove Programs' will now display both 'TANDBERG Content Server Updates' as well as 'TANDBERG Server Appliance Security Updates' after this update is applied. This is due to the name change with the security updates and can be safely ignored.

This update contains updates released from July 2008, for updates prior to this please install 'TSA Security Updates 2008-6'.

**IMPORTANT:** The only supported installation methods is through either the local box (e.g. USB keyboard and monitor locally connected) or through the Microsoft Remote Desktop Utility installed locally on a remote PC. Other utilities, including web-based Remote Desktop Utilities are not supported and should not be used under any circumstances.

## Microsoft Security Updates

### February 2009

The following security updates were released by Microsoft in February 2009 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 961260	<a href="#">Cumulative Security Update for Internet Explorer (961260)</a>
-----------	---

# SOFTWARE RELEASE NOTES FOR TANDBERG SERVER APPLIANCE SECURITY UPDATES 2009-1

## Introduction

These release notes describe the features and capabilities included in the TANDBERG Server Appliance Security Updates software version 2009-1 released on 26 January 2009.

## Security Updates Overview

This version of the Security Updates 2009-1 installs the following Microsoft Security Updates.

This Installer includes Microsoft security updates for TANDBERG Server Appliances with Windows Server 2003 Service Pack 2 installed. Please ensure that the Windows Server Service Pack 2 is installed on the server before proceeding with this installation.

Visit [http://www.tandberg.com/support/tandberg\\_device\\_security.jsp](http://www.tandberg.com/support/tandberg_device_security.jsp) for instructions on how to install Microsoft Windows Service Pack 2 on the TANDBERG Server Appliance.

**Note:** If no updates have been applied to the server since 2008, the program list within 'Add/Remove Programs' will now display both 'TANDBERG Content Server Updates' as well as 'TANDBERG Server Appliance Security Updates' after this update is applied. This is due to the name change with the security updates and can be safely ignored.

This update contains updates released from July 2008, for updates prior to this please install 'TSA Security Updates 2008-6'.

**IMPORTANT:** The only supported installation methods is through either the local box (e.g. USB keyboard and monitor locally connected) or through the Microsoft Remote Desktop Utility installed locally on a remote PC. Other utilities, including web-based Remote Desktop Utilities are not supported and should not be used under any circumstances.

## Microsoft Security Updates

### January 2009

The following security updates were released by Microsoft in January 2009 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 958687	<a href="#">Vulnerabilities in SMB Could Allow Remote Code Execution (958687)</a>
-----------	---

## December 2008

The following security updates were released by Microsoft in December 2008 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 956802	<a href="#">Microsoft Security Bulletin MS08-071 – Critical: Vulnerabilities in GDI Could Allow Remote Code Execution (956802)</a>
KB 958215	<a href="#">Microsoft Security Bulletin MS08-073 - Critical: Cumulative Security Update for Internet Explorer (958215)</a>
KB 959807	<a href="#">Microsoft Security Bulletin MS08-076 – Important: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution (959807)</a>

## November 2008

The following security updates were released by Microsoft in November 2008 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 955218	<a href="#">Microsoft Security Bulletin MS08-069 – Critical: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution (955218)</a>
KB 957097	<a href="#">Microsoft Security Bulletin MS08-068 – Important: Vulnerability in SMB Could Allow Remote Code Execution (957097)</a>

## October 2008 – Out-of-Band Update

The following security updates were released by Microsoft in October 2008 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 958644	<a href="#">Vulnerability in Server Service Could Allow Remote Code Execution (958644)</a>
-----------	--

## October 2008

The following security updates were released by Microsoft in October 2008 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 956390	<a href="#">Cumulative Security Update for Internet Explorer (956390)</a>
KB 956803	<a href="#">Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege (956803)</a>
KB 957095	<a href="#">Vulnerability in SMB Could Allow Remote Code Execution (957095)</a>
KB 956841	<a href="#">Vulnerability in Virtual Address Descriptor Manipulation Could Allow Elevation of Privilege (956841)</a>
KB 954211	<a href="#">Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (954211)</a>

## September 2008

The following security updates were released by Microsoft in September 2008 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 954593	<a href="#">Vulnerabilities in GDI+ Could Allow Remote Code Execution (954593)</a>
KB 954156	<a href="#">Vulnerability in Windows Media Encoder 9 Could Allow Remote Code Execution (954156)</a>

## August 2008

The following security updates were released by Microsoft in August 2008 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 952954	<a href="#">Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution (952954)</a>
KB 953838	<a href="#">Cumulative Security Update for Internet Explorer (953838)</a>
KB 950974	<a href="#">Vulnerabilities in Event System Could Allow Remote Code Execution (950974)</a>
KB 951072	<a href="#">August 2008 cumulative time zone update for Microsoft Windows operating systems</a>

## July 2008

The following security updates were released by Microsoft in July 2008 and apply directly to the Server Appliance. For more information on the security updates themselves, please reference [www.microsoft.com](http://www.microsoft.com) and search for the corresponding KB number.

KB 953230	<a href="#">Vulnerabilities in DNS Could Allow Spoofing (953230)</a>
-----------	--

## Supplemental Notes

### Security Patches

TANDBERG will release a patch specifically for the Server Appliance within one calendar week of Microsoft's patch release. This file will only include relevant patches that need to be applied to the Server Appliance to patch the components the system uses to achieve the TANDBERG specific functionality. All patches released from TANDBERG are tested to ensure there is no effect on functionality from the Server Appliance.

Patches should only be applied through the TANDBERG Security Update as the updates distributed from TANDBERG have been tested to ensure they do not cause issues with the service on the box.

### References/Related Documents

TANDBERG Website – <http://www.tandberg.com>

For all documentation please see the TANDBERG Support Website at:

<http://www.tandberg.com/support/documentation.php>

### Getting the Software

Customers should contact their TANDBERG partner or maintenance provider for support and assistance with their TANDBERG products. Contact your TANDBERG partner or maintenance provider for the software file and release key. The software can be downloaded from TANDBERG's web site at:

[http://www.tandberg.com/support/download\\_software.jsp](http://www.tandberg.com/support/download_software.jsp)

All security patches can be downloaded directly from TANDBERG on the corporate website at [www.tandberg.com/security](http://www.tandberg.com/security). For information regarding the installation of the patches, please contact your authorized TANDBERG support representative.

Previous version: [http://www.tandberg.com/support/tandberg\\_device\\_security.jsp](http://www.tandberg.com/support/tandberg_device_security.jsp)

**Note:** Installation of the patch will require a restart of the Server Appliance to complete the installation.

## Installation of Security Patch

**IMPORTANT:** The only supported installation methods (for both Content Server software and security updates) is through either the local box (e.g. USB keyboard and monitor locally connected) or through the Microsoft Remote Desktop Utility installed locally on a remote PC. Other utilities, including web-based Remote Desktop Utilities are not supported and should not be used under any circumstances. During the installation the TCS must have Internet access to [crl.verisign.com](http://crl.verisign.com) and [Microsoft.com](http://Microsoft.com) certificate revocation lists to validate the certificate on the signed TCS service applications.

1. Download the latest security patch installer from [www.tandberg.com/security](http://www.tandberg.com/security) to the local PC.
2. Copy Security Patch installer to the desktop of the TANDBERG Server Appliance via 'Remote Desktop'.
  - a. Click on 'Start→All Programs →Accessories→Communications→Remote Desktop Connections' and type in the IP address or DNS host name of the Server Appliance. Once the Remote Desktop Connection program opens, click on 'Options >>' to bring up the advanced configuration screen.

**Note:** You may get a 'Remote Desktop connection' security warning, just click 'Ok' to continue.



**Fig 1: Remote Desktop Connection Window**

- b. Under the 'General' tab change the user to 'administrator' and enter the password to the Server Appliance.



**Fig 2: Remote Desktop – General Tab**

- c. Click on the 'Local Resources' tab, un-check 'Printers', check 'Drives', then 'Connect' to establish connection to Server Appliance. This will map the local PC drives to the Server Appliance for this connection, allowing the administrator to easily move files from the local PC to the remote Server Appliance.



**Fig 3: Remote Desktop – Local Resources Tab**

- d. Navigate through 'My Computer' to the mapped drives that reference the current drives on the local PC to the folder that contains the current security patch.
- e. Copy the security patch to the Server Appliance.

**Note:** Do not run the patch over the network connection. To ensure proper installation, copy the patch over to the Appliance Server and then run locally off of the Server Appliance.

- f. Double click on the 'Security Patch Installer.exe' and follow the on-screen instructions.
- g. Once the installer has completed a restart message prompt will appear to restart the Server Appliance for the patch installation to complete.