

1.0 A Message To Our Customers

Hologic, Inc. continues its dedication and commitment to provide the highest quality of products and services to help treat your patients with the best possible experience we can offer. We at Hologic are aware of the threat that malware such as worms and viruses pose. We want you to know about the efforts that we have put forth in evaluating the risks to our products caused by these malicious attacks and software vulnerabilities.

1.1 Hologic's Response to Malicious Attacks, and Malware

Hologic recognizes the need to quickly react to new vulnerabilities that may affect your systems. Of greatest concern to us are "Zero Day" exploits. These are exploits that have not yet been acknowledged by vendors (via a patch or fix method). Hologic has recently introduced a number of actions to deal with existing and future malicious attacks. They include:

- Cybersecurity Team. This team regularly convenes to assess the affect recent security patch releases may have on our products.
- Best Practices Guide to further minimize any harmful exposure. This guide may be found at <http://www.hologic.com/en/product-support/digital-mammography/dsm/>
- On-going monitoring of the industry for software vulnerabilities
- Hologic reviews recently released security patches to access the potential for harm to our products and will test patches that affect our products
- The list of validated patches is published under Product Report and it can be found at <http://www.hologic.com/en/product-support/digital-mammography/dsm/>

2.0 Product Affected

This document pertains to DSM systems on Windows XP SP3.

3.0 Anti-Virus Software

Hologic acknowledges your concern for obtaining virus protection; therefore, we have evaluated the DSM with several anti-virus software solutions. Please see the Anti-virus Installation Instructions for a list of currently supported solutions at <http://www.hologic.com/en/product-support/digital-mammography/dsm/>

Please contact your Hologic service representative for assistance with installation of these products. Instructions for installing and configuring ant-virus can be found in the guide entitled Anti-virus Installation Instructions.

4.0 Operating System Updates and Security Patches

Hologic performs risk analysis to determine the potential consequences of software vulnerability. We also analyze any risk to the system from applying a security patch. DSM is FDA approved medical device therefore only Hologic validated security patches should be applied as un-tested patches can have adverse effect on the system. If you install these security patches, please follow the Customer Validation Form provided to ensure the DSM operates correctly.

**Note...**

Hologic lists all validated patches that are applicable to the DSM. If a patch appears to be missing from the list, it isn't applicable to DSM. Please contact your Hologic Customer Service Representative for further assistance.

A list of Microsoft patches have been validated to work with DSM. Please see the patch depositions table starting on page 5 for detail.

4.1 Installing Patches

**Note...**

Ensure the system has access to Microsoft's update webpage before proceeding or download validated patches through another mechanism then install and skip to 5.0.

1. On the DSM, login to Windows as **Customer**.
2. Installation procedures:
3. Browse to <http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us>
4. A pop-up may appear, click **Accept**.
5. When the website is displayed, click **Custom install**. The Windows Update page will scan for available patches for your system
6. If a message is displayed saying "We've made upgrades" click "Download" and proceed as described in step C
7. After the page has found the available patches, click High-priority on the left window
8. Ensure that the patches that are selected have been approved by Hologic before proceeding. Uncheck any patches that are not on the approval list.
9. Click **Review and Install updates**.
10. Click **Install Updates**. Select **Client install** and proceed to the next window.
11. If windows appear prompting with questions, click **Accept**.
12. After the patches have been downloaded, reboot the system.

**Note...**

If the system does not have direct access to Microsoft's update webpage, download the update from a separate PC and transport them over for installation on the vulnerable system.

5.0 Customer Validation Test

This test should be conducted as an additional step to ensure system stability was not compromised due to patch installation.

**Note...**

This test is to ONLY be used for patches that have been validated by Hologic. You are not permitted to use this validation form to perform validation on non-validated Hologic patches.

5.1 Re-boot and Restart the DSM Software

If any patches were applied, shutdown the computer and restart the DSM software. Use the normal customer Log-on (User Name: **dsm**).

5.2 Check Basic System Operation

1. Select *Directory List* from the DSM main menu. Verify that the list of cases is displayed correctly.
2. Recall a case study. Verify that the images in the case are recalled correctly.
3. Acquire a Stereo Pair using the StereoGuide/MultiCare calibration needle as a target. Place the needle at X=10mm, Y=20mm, Z=30mm using the procedures outlined in the operator manual.
4. If the X-ray machine has a video monitor, verify that the patient demographics (Patient ID, Patient Name, etc.) is displayed correctly at the X-ray console during the acquire sequence.
5. Select *Stereo Target*. Mark the tip of the needle in both images. Verify that the correct XYZ values are displayed in the Stereo Targeting dialog box.
6. Transmit the XYZ values to the Needle Stage. Verify that the values were transmitted correctly.

5.3 Check DICOM Operation (if applicable)

1. Select *File Manager* from the DSM main menu. Verify that the list of images is displayed correctly.
2. Use the *Print Film* function to print a case study to the DICOM printer. Verify that the images are printed correctly.
3. Use the File Manager *Copy* function to copy a case study to the DICOM Storage Server. Verify that no errors occur. (Use the images that were acquired in the Check Basic System Operation section above).
4. Use the File Manager *Erase* function to erase the case study that was copied to the Storage Server in step 3 from the hard drive.
5. Use the *DICOM Query* function to retrieve the case study back to the DSM system. Verify that no errors occur.
6. Select *Directory List* from the DSM main menu. Recall the case study that was retrieved in step 5. Verify that the images in the case study are recalled correctly.

6.0 Questions and Concerns

Hologic is here to help. We understand you have both a financial responsibility and operational responsibility to protect your networks and computer systems from malicious harm. If you have any questions or concerns, please contact your Hologic Sales or Service Representative.

Table 1: Patch dispositions

Patch	Description	Link	Disposition
MS08-032	Cumulative Security Update of ActiveX Kill Bits	http://www.microsoft.com/technet/security/bulletin/MS08-032.mspx	Validated
MS08-036	Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service	http://www.microsoft.com/technet/security/bulletin/MS08-036.mspx	Validated
MS08-037	Vulnerabilities in DNS Could Allow Spoofing	http://www.microsoft.com/technet/security/bulletin/MS08-037.mspx	Validated
MS08-046	Vulnerability in Microsoft Windows Image Color Management System Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-046.mspx	Validated
MS08-048	Security Update for Outlook Express and Windows Mail	http://www.microsoft.com/technet/security/bulletin/MS08-048.mspx	Validated
MS08-049	Vulnerabilities in Event System Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-049.mspx	Validated
MS08-062	Vulnerability in Windows Internet Printing Service Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-062.mspx	Validated
MS08-066	Vulnerability in the Microsoft Ancillary Function Driver Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS08-066.mspx	Validated
MS08-067	Vulnerability in Server Service Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx	Validated
MS08-068	Vulnerability in SMB Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-068.mspx	Validated
MS08-069	Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-069.mspx	Validated
MS08-071	Vulnerabilities in GDI Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-071.mspx	Validated
MS08-076	Vulnerabilities in Windows Media Components Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms08-076.mspx	Validated
MS09-001	Vulnerabilities in SMB Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-001.mspx	Validated
MS09-007	Vulnerability in SChannel Could Allow Spoofing	http://www.microsoft.com/technet/security/bulletin/MS09-007.mspx	Validated

Patch	Description	Link	Disposition
MS09-010	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-010.msp	Validated
MS09-012	Vulnerabilities in Windows Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-012.msp	Validated
MS09-013	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-013.msp	Validated
MS09-015	Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-015.msp	Validated
MS09-022	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-022.msp	Validated
MS09-026	Vulnerability in RPC Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-026.msp	Validated
MS09-028	Vulnerabilities in Microsoft DirectShow Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-028.msp	Validated
MS09-037	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-037.msp	Validated
MS09-038	Vulnerabilities in Windows Media File Processing Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-038.msp	Validated
MS09-041	Vulnerability in Workstation Service Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-041.msp	Validated
MS09-042	Vulnerability in Telnet Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-042.msp	Validated
MS09-044	Vulnerabilities in Remote Desktop Connection Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-044.msp	Validated
MS09-045	Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-045.msp	Validated
MS09-046	Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-046.msp	Validated
MS09-051	Vulnerabilities in Windows Media Runtime Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-051.msp	Validated

Patch	Description	Link	Disposition
MS09-052	Vulnerability in Windows Media Player Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-052.mspx	Validated
MS09-055	Cumulative Security Update of ActiveX Kill Bits	http://www.microsoft.com/technet/security/bulletin/MS09-055.mspx	Validated
MS09-056	Vulnerabilities in Windows CryptoAPI Could Allow Spoofing	http://www.microsoft.com/technet/security/bulletin/MS09-056.mspx	Validated
MS09-057	Vulnerability in Indexing Service Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-057.mspx	Validated
MS09-058	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-058.mspx	Validated
MS09-059	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service	http://www.microsoft.com/technet/security/bulletin/MS09-059.mspx	Validated
MS09-062	Vulnerabilities in GDI+ Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-062.mspx	Validated
MS09-065	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-065.mspx	Validated
MS09-069	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service	http://www.microsoft.com/technet/security/bulletin/MS09-069.mspx	Validated
MS09-071	Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-071.mspx	Validated
MS09-072	Cumulative Security Update for Internet Explorer	http://www.microsoft.com/technet/security/bulletin/MS09-072.mspx	Validated
MS09-073	Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-073.mspx	Validated
MS10-001	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-001.mspx	Validated
MS10-002	Cumulative Security Update for Internet Explorer	http://www.microsoft.com/technet/security/bulletin/MS10-002.mspx	Validated
MS10-005	Vulnerability in Microsoft Paint Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-005.mspx	Validated

Patch	Description	Link	Disposition
MS10-007	Vulnerability in Windows Shell Handler Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-007.msp	Validated
MS10-011	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS10-011.msp	Validated
MS10-013	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-013.msp	Validated
MS10-019	Vulnerabilities in Windows Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-019.msp	Validated
MS10-020	Vulnerabilities in SMB Client Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-020.msp	Validated
MS10-022	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-022.msp	Validated
MS10-026	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-026.msp	Validated
MS10-027	Vulnerability in Windows Media Player Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-027.msp	Validated
MS10-029	Vulnerability in Windows ISATAP Component Could Allow Spoofing	http://www.microsoft.com/technet/security/bulletin/MS10-029.msp	Validated
MS10-030	Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-030.msp	Validated
MS10-033	Vulnerabilities in Media Decompression Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-033.msp	Validated
MS10-034	Cumulative Security Update of ActiveX Kill Bits	http://www.microsoft.com/technet/security/bulletin/MS10-034.msp	Validated
MS10-037	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS10-037.msp	Validated
MS10-041	Vulnerability in Microsoft .NET Framework Could Allow Tampering	http://www.microsoft.com/technet/security/bulletin/MS10-041.msp	Validated
MS10-042	Vulnerability in Help and Support Center Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-042.msp	Validated

Patch	Description	Link	Disposition
MS10-046	Vulnerability in Windows Shell Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-046.aspx	Validated
MS10-047	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS10-047.aspx	Validated
MS10-048	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS10-048.aspx	Validated
MS10-049	Vulnerabilities in SChannel could allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-049.aspx	Validated
MS10-051	Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-051.aspx	Validated
MS10-052	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-052.aspx	Validated
MS10-053	Cumulative Security Update for Internet Explorer	http://www.microsoft.com/technet/security/bulletin/MS10-053.aspx	Validated
MS10-054	Vulnerabilities in SMB Server Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-054.aspx	Validated
MS10-055	Vulnerability in Cinepak Codec Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-055.aspx	Validated
MS10-060	Vulnerabilities in the Microsoft .NET Common Language Runtime and in Microsoft Silverlight Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-060.aspx	Validated
MS10-061	Vulnerability in Print Spooler Service Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-061.aspx	Validated
MS10-063	Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-063.aspx	Validated
MS10-066	Vulnerability in Remote Procedure Call Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-066.aspx	Validated
MS10-067	Vulnerability in WordPad Text Converters Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-067.aspx	Validated
MS10-069	Vulnerability in Windows Client/Server Runtime Subsystem Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms10-069.aspx	Validated

Patch	Description	Link	Disposition
MS10-070	Vulnerability in ASP.NET Could Allow Information Disclosure	http://www.microsoft.com/technet/security/bulletin/ms10-070.msp	Validated
MS10-073	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms10-073.msp	Validated
MS10-074	Vulnerability in Microsoft Foundation Classes Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-074.msp	Validated
MS10-076	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-076.msp	Validated
MS10-078	Vulnerabilities in the OpenType Font (OTF) Format Driver Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms10-078.msp	Validated
MS10-081	Vulnerability in Windows Common Control Library Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-081.msp	Validated
MS10-082	Vulnerability in Windows Media Player Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-082.msp	Validated
MS10-083	Vulnerability in COM Validation in Windows Shell and WordPad Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-083.msp	Validated
MS10-084	Vulnerability in Windows Local Procedure Call Could Cause Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms10-084.msp	Validated
MS10-097	Insecure Library Loading in Internet Connection Signup Wizard Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms10-097.msp	Validated
MS10-099	Vulnerability in Routing and Remote Access Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms10-099.msp	Validated
MS11-002	Vulnerabilities in Microsoft Data Access Components Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-002.msp	Validated
MS11-006	Vulnerability in Windows Shell Graphics Processing Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-006.msp	Validated
MS11-011	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-011.msp	Validated
MS11-012	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-012.msp	Validated

Patch	Description	Link	Disposition
MS11-013	Vulnerabilities in Kerberos Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-013.mspx	Validated
MS11-014	Vulnerability in Local Security Authority Subsystem Service Could Allow Local Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-014.mspx	Validated
MS11-015	Vulnerabilities in Windows Media Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-015.mspx	Validated
MS11-017	Vulnerability in Remote Desktop Client Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-017.mspx	Validated
MS11-020	Vulnerability in SMB Server Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-020.mspx	Validated
MS11-024	Vulnerabilities in Windows Fax Cover Page Editor Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-024.mspx	Validated
MS11-027	Cumulative Security Update of ActiveX Kill Bits	http://www.microsoft.com/technet/security/bulletin/ms11-027.mspx	Validated
MS11-029	Vulnerability in GDI+ Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-029.mspx	Validated
MS11-030	Vulnerability in DNS Resolution Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-030.mspx	Validated
MS11-031	Vulnerability in JScript and VBScript Scripting Engines Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-031.mspx	Validated
MS11-032	Vulnerability in the OpenType Compact Font Format (CFF) Driver Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-032.mspx	Validated
MS11-033	Vulnerability in WordPad Text Converters Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-033.mspx	Validated
MS11-037	Vulnerability in MHTML Could Allow Information Disclosure	http://www.microsoft.com/technet/security/bulletin/ms11-037.mspx	Validated
MS11-038	Vulnerability in OLE Automation Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-038.mspx	Validated
MS11-042	Vulnerabilities in Distributed File System Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-042.mspx	Validated

Patch	Description	Link	Disposition
MS11-043	Vulnerability in SMB Client Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-043.msp	Validated
MS11-044	Vulnerability in .NET Framework Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-044.msp	Validated
MS11-046	Vulnerability in Ancillary Function Driver Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-046.msp	Validated
MS11-052	Vulnerability in Vector Markup Language Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/ms11-052.msp	Validated
MS11-054	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-054.msp	Validated
MS11-056	Vulnerabilities in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-056.msp	Validated
MS11-057	Cumulative Security Update for Internet Explorer	http://www.microsoft.com/technet/security/bulletin/ms11-057.msp	Validated
MS11-062	Vulnerability in Remote Access Service NDISTAPI Driver Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-062.msp	Validated
MS11-063	Vulnerability in Windows Client/Server Run-time Subsystem Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/ms11-063.msp	Validated
MS11-065	Vulnerability in Remote Desktop Protocol Could Allow Denial of Service	http://www.microsoft.com/technet/security/bulletin/ms11-065.msp	Validated
MS11-069	Vulnerability in .NET Framework Could Allow Information Disclosure	http://www.microsoft.com/technet/security/bulletin/ms11-069.msp	Validated