

DSM Cyber-Security Product Report

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 computer vulnerabilities.

Hologic's Response to Malicious Attacks, Virus, 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 assess 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 the following product:

- DSM systems on Windows 2000 SP4

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 anti-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. Please note this is the last patch validation for DSM on Windows 2000 as the operating system has reached end of life and patches is no longer released by Microsoft. Please upgrade to the new DSM running on Windows XP SP3 for continued security maintenance.

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

- a. On the DSM, login to Windows as **ntdsm**.
- b. Installation procedures:
- c. Browse to <http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us>
- d. A pop-up may appear, click Accept.
- e. When the website is displayed, click Custom install. The Windows Update page will scan for available patches for your system
- f. If a message is displayed saying "We've made upgrades" click "Download" and proceed as described in step C
- g. After the page has found the available patches, click High-priority on the left window
- h. Ensure that the patches that are selected have been approved by Hologic before proceeding. Uncheck any patches that are not on the approval list.
- i. Click Review and Install updates.
- j. Click Install Updates. Select Client install and proceed to the next window.
- k. If windows appear prompting with questions, click Accept.
- l. 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.

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).

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.

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.

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.

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.

Patch dispositions

Patch	Description	Link	Disposition
	Service Pack 4 (Hologic Installed Only)	http://www.microsoft.com/windows2000/downloads/servicepacks/sp4/	Validated
MS04-016	Vulnerability in DirectPlay could allow denial of service	http://support.microsoft.com/?kbid=839643	Validated
	An update package that includes BITS 2.0 and WinHTTP 5.1 is available for Windows Server 2003, for Windows XP, and for Windows 2000	http://support.microsoft.com/?kbid=842773	Validated
MS05-014	Cumulative security update for Internet Explorer	http://support.microsoft.com/?kbid=867282	Validated
MS05-020	Cumulative security update for Internet Explorer	http://support.microsoft.com/?kbid=890923	Validated
MS05-024	Vulnerability in Web View could allow remote code execution	http://support.microsoft.com/?kbid=894320	Validated
MS05-026	A vulnerability in HTML Help could allow remote code execution	http://support.microsoft.com/?kbid=896358	Validated
MS05-027	Vulnerability in Server Message Block could allow remote code execution	http://support.microsoft.com/?kbid=896422	Validated
MS05-030	Vulnerability in Outlook Express could allow remote code execution	http://support.microsoft.com/?kbid=897715	Validated
MS05-032	Vulnerability in Microsoft agent could allow spoofing	http://support.microsoft.com/?kbid=890046	Validated
MS05-036	Vulnerability in Microsoft Color Management Module could allow remote code execution	http://support.microsoft.com/?kbid=901214	Validated
MS05-040	Vulnerability in Telephony service could allow remote code execution	http://support.microsoft.com/?kbid=893756	Validated
MS05-043	Vulnerability in Print Spooler service could allow remote code execution	http://support.microsoft.com/?kbid=896423	Validated
	Vulnerability in the Microsoft Collaboration Data Objects could allow code execution (Windows)	http://support.microsoft.com/?kbid=901017	Validated
MS05-044	Vulnerability in the Windows FTP client could allow file transfer location tampering	http://support.microsoft.com/?kbid=905495	Validated
MS05-045	Vulnerability in Network Connection Manager could allow denial of service	http://support.microsoft.com/?kbid=905414	Validated
MS05-046	Vulnerability in the Client Service for NetWare could allow remote code execution	http://support.microsoft.com/?kbid=899589	Validated
MS05-047	Vulnerability in Plug and Play could allow remote code execution and local elevation of privilege	http://support.microsoft.com/?kbid=905749	Validated
MS05-049	Vulnerabilities in the Windows shell .could allow for remote code execution	http://support.microsoft.com/?kbid=900725	Validated
MS05-050	Vulnerability in DirectShow could allow remote code execution	http://www.microsoft.com/technet/security/Bulletin/MS05-050.mspx	Validated
MS05-051	Vulnerabilities in MS DTC and COM+ could allow remote code execution	http://support.microsoft.com/?kbid=902400	Validated
MS05-052	Cumulative security update for Internet Explorer	http://support.microsoft.com/?kbid=896688	Validated
MS05-053	Vulnerabilities in graphics rendering engine could allow code execution	http://support.microsoft.com/?kbid=896424	Validated
MS05-055	Vulnerability in Windows kernel could allow elevation of privilege	http://support.microsoft.com/?kbid=908523	Validated
MS06-001	Vulnerability in graphics rendering engine could allow remote code execution	http://support.microsoft.com/?kbid=912919	Validated
MS06-002	Vulnerability in embedded Web fonts could allow remote code execution	http://support.microsoft.com/?kbid=908519	Validated

Patch	Description	Link	Disposition
MS06-014	Vulnerability in Microsoft Data Access Components (MDAC) function could allow code execution	http://support.microsoft.com/?kbid=911562	Validated
MS06-015	Vulnerability in Windows Explorer Could Lead to Remote Code Execution	http://support.microsoft.com/?kbid=908531	Validated
MS06-057	Vulnerability in Windows Explorer could allow remote code execution	http://www.microsoft.com/technet/security/Bulletin/MS06-057.msp	Validated
MS06-061	Vulnerabilities in Microsoft XML Core Services could allow remote code execution	http://www.microsoft.com/technet/security/Bulletin/MS06-061.msp	Validated
MS06-063	Vulnerability in Server Service could allow denial of service	http://www.microsoft.com/technet/security/Bulletin/MS06-063.msp	Validated
MS06-066	Vulnerability in the Client Service could allow remote code execution	http://www.microsoft.com/technet/security/Bulletin/MS06-066.msp	Validated
MS06-068	Vulnerability in Microsoft Agent could allow remote code execution	http://www.microsoft.com/technet/security/Bulletin/MS06-068.msp	Validated
MS06-070	Vulnerability in Workstation Service could allow remote code execution	http://www.microsoft.com/technet/security/Bulletin/MS06-070.msp	Validated
MS06-071	Security update for Microsoft XML Core Services 4.0	http://www.microsoft.com/technet/security/Bulletin/MS06-071.msp	Validated
MS06-072	Cumulative security update for Internet Explorer	http://www.microsoft.com/technet/security/Bulletin/MS06-072.msp	Validated
MS06-076	Cumulative security update for Outlook Express	http://www.microsoft.com/technet/security/Bulletin/MS06-076.msp	Validated
MS06-078	Vulnerability in Windows Media Format could allow remote code execution	http://www.microsoft.com/technet/security/Bulletin/MS06-078.msp	Validated
	Windows Installer 3.1 v2 (3.1.4000.2435) is available	http://support.microsoft.com/?kbid=893803	Validated
	Update for Windows Media Player URL script command behavior	http://support.microsoft.com/?kbid=828026	Validated
MS07-008	Vulnerability in HTML Help ActiveX Control Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-008.msp	Validated
MS07-009	Vulnerability in Microsoft Data Access Components Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-009.msp	Validated
MS07-011	Vulnerability in Microsoft OLE Dialog Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-011.msp	Validated
MS07-012	Vulnerability in Microsoft MFC Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-012.msp	Validated
MS07-013	Vulnerability in Microsoft RichEdit Could Allow Remote Code	http://www.microsoft.com/technet/security/bulletin/MS07-013.msp	Validated
MS07-017	Vulnerabilities in GDI Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-017.msp	Validated
MS07-021	Vulnerabilities in CSRSS Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-021.msp	Validated
MS07-022	Vulnerability in Windows Kernel Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS07-022.msp	Validated
MS07-031	Vulnerability in the Windows Schannel Security Package Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-031.msp	Validated

Patch	Description	Link	Disposition
MS07-035	Vulnerability in Win 32 API Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-035.mspx	Validated
MS07-050	Vulnerability in Vector Markup Language Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-050.mspx	Validated
MS07-051	Vulnerability in Microsoft Agent Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-051.mspx	Validated
MS07-055	Vulnerability in Kodak Image Viewer Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-055.mspx	Validated
MS07-058	Vulnerability in RPC Could Allow Denial of Service	http://www.microsoft.com/technet/security/bulletin/MS07-058.mspx	Validated
MS07-064	Vulnerabilities in DirectX Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-064.mspx	Validated
MS07-065	Vulnerability in Message Queuing Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS07-065.mspx	Validated
MS08-002	Professional Vulnerability in LSASS Could Allow Local Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS08-002.mspx	Validated
MS08-008	Vulnerability in OLE Automation Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-008.mspx	Validated
MS08-020	Vulnerability in DNS Client Could Allow Spoofing	http://www.microsoft.com/technet/security/bulletin/MS08-020.mspx	Validated
MS08-022	Vulnerability in VBScript and JScript Scripting Engines Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-022.mspx	Validated
MS08-023	Internet Explorer 6 Security Update of ActiveX Kill Bits	http://www.microsoft.com/technet/security/bulletin/MS08-023.mspx	Validated
MS08-028	Vulnerability in Microsoft Jet Database Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-028.mspx	Validated
MS08-032	Cumulative Security Update of ActiveX Kill Bits	http://www.microsoft.com/technet/security/bulletin/MS08-032.mspx	Validated
MS08-033	Vulnerabilities in DirectX Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-033.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
MS08-052	Vulnerabilities in GDI+ Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-052.mspx	Validated
MS08-061	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS08-061.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	
MS08-067	Vulnerability in Server Service Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx	Validated

Patch	Description	Link	Disposition
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
MS08-073	Internet Explorer 6 Cumulative Security Update for Internet Explorer	http://www.microsoft.com/technet/security/bulletin/MS08-073.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
MS08-078	Internet Explorer 6 Security Update for Internet Explorer	http://www.microsoft.com/technet/security/bulletin/MS08-078.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
MS09-010	Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-010.mspx	Validated
MS09-012	Vulnerabilities in Windows Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-012.mspx	Validated
MS09-013	Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-013.mspx	Validated
MS09-015	Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-015.mspx	Validated
MS09-022	Vulnerabilities in Windows Print Spooler Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-022.mspx	Validated
MS09-026	Vulnerability in RPC Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS09-026.mspx	Validated
MS09-037	Vulnerabilities in Microsoft Active Template Library (ATL) Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-037.mspx	Validated
MS09-042	Vulnerability in Telnet Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-042.mspx	Validated
MS09-045	Vulnerability in JScript Scripting Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-045.mspx	Validated
MS09-046	Vulnerability in DHTML Editing Component ActiveX Control Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-046.mspx	Validated
MS09-052	Vulnerability in Windows Media Player Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-052.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

Patch	Description	Link	Disposition
MS09-062	Vulnerabilities in GDI+ Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-062.mspix	Validated
MS09-069	Vulnerability in Local Security Authority Subsystem Service Could Allow Denial of Service	http://www.microsoft.com/technet/security/bulletin/MS09-069.mspix	Validated
MS09-071	Vulnerabilities in Internet Authentication Service Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-071.mspix	Validated
MS09-073	Vulnerability in WordPad and Office Text Converters Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS09-073.mspix	Validated
MS10-001	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-001.mspix	Validated
MS10-005	Vulnerability in Microsoft Paint Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-005.mspix	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.mspix	Validated
MS10-012	Vulnerabilities in SMB Server Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-012.mspix	Validated
MS10-013	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-013.mspix	Validated
MS10-019	Vulnerabilities in Windows Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-019.mspix	Validated
MS10-020	Vulnerabilities in SMB Client Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-020.mspix	Validated
MS10-021	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS10-021.mspix	Validated
MS10-022	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-022.mspix	Validated
MS10-026	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-026.mspix	Validated
MS10-030	Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-030.mspix	Validated
MS10-032	Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	http://www.microsoft.com/technet/security/bulletin/MS10-032.mspix	Validated
MS10-033	Vulnerabilities in Media Decompression Could Allow Remote Code Execution	http://www.microsoft.com/technet/security/bulletin/MS10-033.mspix	Validated
MS10-034	Cumulative Security Update of ActiveX Kill Bits	http://www.microsoft.com/technet/security/bulletin/MS10-034.mspix	Validated
MS10-035	Cumulative Security Update for Internet Explorer	http://www.microsoft.com/technet/security/bulletin/MS10-035.mspix	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.mspix	Validated