

Artwork and Signature File for:

MAN-00558, "MIMS v.1.2 Cybersecurity Product Report"

Artwork consists of:

- Ten (10) 8 ½ inch x 11 inch pages.

REV AUTHORED BY W. TANG	DATE 07/01/09	HOLOGIC ® A FAMILY OF COMPANIES	Osteoporosis Assessment LORAD® Breast Cancer Detection DirectRay® Digital Imaging FLUOROSCAN® C-arm Imaging	SIGNATURES ON FILE
REV DRAFTED BY W. TANG	DATE 07/01/09			
PROPRIETARY: This document contains proprietary data of Hologic, Inc. No disclosure, reproduction or use of any part thereof may be made except by written permission from Hologic.		TITLE MIMS v.1.2 Cybersecurity Product Report	DOCUMENT NUMBER AW-01434	REV 008
REV. RELEASE DATE:	07/13/09	ARTWORK	SIZE A	SHEET 1 OF 1

MIMS v1.2 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 malicious users and malware may pose to your IT infrastructure. We want you to know about the efforts that we have put forth in evaluating the risks to our products caused by malware and the countermeasures we take to combat them.

Hologic's Response to Malicious Attacks, Viruses and Malware

Hologic recognizes the need to react quickly 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:

- Creation of a *Cyber Security Team*. This team regularly convenes to assess the effect recent security patch releases may have on our products.
- Release of a *Best Practices Guide* to further minimize any harmful exposure.
- On-going monitoring of the information security industry for new vulnerabilities.
- Periodic Vulnerability Assessments on Hologic products.

2.0 Products Affected

This document pertains to the following Hologic MIMS product:

- **MIMS running on Windows 2003 Server SP1 or SP2**

3.0 Anti-Virus

Hologic acknowledges your concern for obtaining anti-virus protection. Therefore, we have evaluated MIMS with several commercial anti-virus products. Please review the "Anti-virus installation instructions" document specific for each product at <http://www.hologic.com/product-support-link/overview/>

Please contact your Hologic Customer Service Representative for assistance with installation of these products if you have any questions. Please ensure that you follow our installation and configuration guide to ensure optimal performance and security.

We strongly encourage customers to use only anti-virus products that we have officially validated, to ensure the continual safety and reliability of our medical related product in order to provide optimal patient care. However, if you insist on using an untested anti-virus solution, you use it at

your own risk. In the event of system corruption, Hologic will restore the system to the factory default state and will charge for time and materials.

4.0 Operating System Updates and Security Patches

Hologic performs risk analysis to determine the potential consequences of published exploits. We also analyze any risk to the system from applying a security patch. Your MIMS is a medical device and as such, recommended security patches are validated by Hologic for effectiveness. Only Hologic validated security patches should be installed on your MIMS. If you install these security patches, please follow the Customer Validation Form provided to ensure the MIMS operates properly after installation. Service Packs must be installed and validated by Hologic and cannot be customer validated.

NOTE: Hologic lists all validated patches that are applicable to the MIMS v1.2. If a patch appears to be missing from the list, it is either not applicable to the system or is currently undergoing validation. Please contact your Hologic Customer Service Representative for further assistance.

These security patches issued in the following Microsoft bulletins have been validated to work with MIMS running on Windows 2003 Server SP1 or SP2:

MS03-023: Buffer overrun in the HTML converter could allow code execution
<http://support.microsoft.com/kb/823559>

MS03-034: Flaw in NetBIOS could lead to information disclosure
<http://support.microsoft.com/kb/824105>

MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution
<http://support.microsoft.com/kb/823182>

MS03-043: Buffer overrun in Messenger service could allow code execution
<http://support.microsoft.com/kb/828035>

MS04-003: Buffer overrun in an MDAC function could allow code execution
<http://support.microsoft.com/kb/832483>

MS04-011: Security Update for Microsoft Windows
<http://support.microsoft.com/kb/835732>

MS04-014: Vulnerability in the Microsoft Jet Database Engine could permit code execution
<http://support.microsoft.com/kb/837001>

MS04-015 Security Update for Microsoft Windows

<http://support.microsoft.com/kb/840374>

MS04-016: Vulnerability in DirectPlay could allow denial of service

<http://support.microsoft.com/kb/839643>

MS04-024: A vulnerability in the Windows shell could allow remote code execution

<http://support.microsoft.com/kb/839645>

MS04-028: Buffer overrun in JPEG processing (GDI+) could allow code execution

<http://support.microsoft.com/kb/833987>

MS04-030: Vulnerability in WebDAV XML message handler could lead to a denial of service

<http://support.microsoft.com/kb/824151>

MS04-031: Vulnerability in NetDDE could allow remote code execution

<http://support.microsoft.com/kb/841533>

MS04-032: Security update for Microsoft Windows

<http://support.microsoft.com/kb/840987>

MS04-034: Vulnerability in compressed (zipped) folders could allow code execution

<http://support.microsoft.com/kb/873376>

MS04-035: Vulnerability in SMTP could allow remote code execution in Microsoft Windows Server 2003

<http://support.microsoft.com/kb/885881>

MS04-036: Vulnerability in NNTP could allow code execution

<http://support.microsoft.com/kb/883935>

MS04-037: Vulnerability in Windows shell could allow remote code execution

<http://support.microsoft.com/kb/841356>

MS04-041: A vulnerability in WordPad could allow code execution

<http://support.microsoft.com/kb/885836>

MS04-043: Vulnerability in HyperTerminal could allow code execution

<http://support.microsoft.com/kb/873339>

MS04-044: Vulnerabilities in Windows Kernel and LSASS could allow elevation of privilege

<http://support.microsoft.com/kb/885835>

MS04-045: Vulnerability in WINS could allow remote code execution

<http://support.microsoft.com/kb/870763>

MS05-002: Vulnerability in cursor and icon format handling could allow remote code execution

<http://support.microsoft.com/kb/891711>

MS05-003: Vulnerability in the Indexing Service could allow remote code execution

<http://support.microsoft.com/kb/871250>

MS05-010: Vulnerability in the License Logging service could allow code execution

<http://support.microsoft.com/kb/885834>

MS05-011: Vulnerability in server message block could allow remote code execution

<http://support.microsoft.com/kb/885250>

MS05-013: Vulnerability in the DHTML editing component ActiveX control could allow code execution

<http://support.microsoft.com/kb/891781>

MS05-015: Vulnerability in hyperlink object library could allow remote code execution in Windows Server 2003

<http://support.microsoft.com/kb/888113>

MS05-018: Vulnerabilities in Windows kernel could allow elevation of privilege and denial of service

<http://support.microsoft.com/kb/890859>

MS05-020: Cumulative security update for Internet Explorer

<http://support.microsoft.com/kb/890923>

MS05-026: A vulnerability in HTML Help could allow remote code execution

<http://support.microsoft.com/kb/896358>

MS05-027: Vulnerability in Server Message Block could allow remote code execution

<http://support.microsoft.com/kb/896422>

MS05-032: Vulnerability in Microsoft agent could allow spoofing

<http://support.microsoft.com/kb/890046>

MS05-033: Vulnerability in Telnet client could allow information disclosure

<http://support.microsoft.com/kb/896428>

MS05-036: Vulnerability in Microsoft Color Management Module could allow remote code execution

<http://support.microsoft.com/kb/901214>

MS05-039: Vulnerability in Plug and Play could allow remote code execution and elevation of privilege

<http://support.microsoft.com/kb/899588>

MS05-040: Vulnerability in Telephony service could allow remote code execution

<http://support.microsoft.com/kb/893756>

MS05-042: Vulnerabilities in Kerberos could allow denial of service, information disclosure, and spoofing

<http://support.microsoft.com/kb/899587>

MS05-041: Vulnerability in Remote Desktop Protocol could allow denial of service

<http://support.microsoft.com/kb/899591>

MS05-043: Vulnerability in Print Spooler service could allow remote code execution

<http://support.microsoft.com/kb/896423>

MS05-044: Vulnerability in the Windows FTP client could allow file transfer location tampering

<http://support.microsoft.com/kb/905495>

MS05-045: Vulnerability in Network Connection Manager could allow denial of service

<http://support.microsoft.com/kb/905414>

MS05-046: Vulnerability in the Client Service for NetWare could allow remote code execution

<http://support.microsoft.com/kb/899589>

Vulnerability in the Microsoft Collaboration Data Objects could allow code execution (Windows)

<http://support.microsoft.com/kb/901017>

MS05-049: Vulnerabilities in the Windows shell could allow for remote code execution

<http://support.microsoft.com/kb/900725>

MS05-050: Vulnerability in DirectShow could allow remote code execution

<http://support.microsoft.com/kb/904706>

MS05-051: Vulnerabilities in MS DTC and COM+ could allow remote code execution

<http://support.microsoft.com/kb/902400>

MS05-053: Vulnerabilities in graphics rendering engine could allow code execution

<http://support.microsoft.com/kb/896424>

MS06-001: Vulnerability in graphics rendering engine could allow remote code execution

<http://support.microsoft.com/kb/912919>

MS06-002: Vulnerability in embedded Web fonts could allow remote code execution

<http://support.microsoft.com/kb/908519>

MS06-005: Vulnerability in Windows Media Player could allow remote code execution

<http://support.microsoft.com/kb/911565>

MS06-006: Vulnerability in Windows Media Player plug-in with non-Microsoft Internet browsers could allow remote code execution

<http://support.microsoft.com/kb/911564>

MS06-007: Vulnerability in TCP/IP could allow denial of service

<http://support.microsoft.com/kb/913446>

MS06-008: Vulnerability in WebClient could allow remote code execution

<http://support.microsoft.com/kb/911927>

MS06-009: Vulnerability in the Korean Input Method Editor (IME) could allow elevation of privilege

<http://support.microsoft.com/kb/901190>

MS06-011: Permissive Windows services DACLs could lead to elevation of privilege

<http://support.microsoft.com/kb/914798>

MS06-013: Cumulative security update for Internet Explorer

<http://support.microsoft.com/kb/912812>

MS06-014: Vulnerability in Microsoft Data Access Components (MDAC) function could allow code execution

<http://support.microsoft.com/kb/911562>

MS06-015: Vulnerability in Windows Explorer Could Lead to Remote Code Execution

<http://support.microsoft.com/kb/908531>

MS06-016: Cumulative Security Update for Outlook Express

<http://support.microsoft.com/kb/911567>

MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinator could allow denial of service

<http://support.microsoft.com/kb/913580>

MS06-035: Vulnerability in Server Service Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/ms06-035.mspx>

MS06-036: Vulnerability in DHCP Client Service Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/ms06-036.mspx>

MS06-040: Vulnerability in Server Service Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx>

MS06-041: Vulnerability in DNS Resolution Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/ms06-041.mspx>

MS06-045: Vulnerability in Windows Explorer Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/ms06-045.mspx>

MS06-051: Vulnerability in Windows Kernel Could Result in Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/ms06-051.mspx>

MS06-057: Vulnerability in Windows Explorer Could Allow Remote Execution
<http://www.microsoft.com/technet/security/Bulletin/MS06-057.mspx>

MS06-063: Vulnerability in Server Service Could Allow Denial of Service
<http://www.microsoft.com/technet/security/Bulletin/MS06-063.mspx>

MS06-064: Vulnerability in TCP/IP IPV6 Could Allow Denial of Service
<http://www.microsoft.com/technet/security/Bulletin/MS06-064.mspx>

MS07-017: Vulnerability in GDI Could Allow Remote Code Execution
<http://support.microsoft.com/kb/925902>

MS07-019: Vulnerability in UNPN Could Allow Remote Code Execution
<http://support.microsoft.com/kb/931261>

MS07-020: Vulnerability in Microsoft Agent Could Allow Remote Code Execution
<http://support.microsoft.com/kb/932168>

MS07-035: Vulnerability in WIN32 API Could Allow Remote Code Execution
<http://support.microsoft.com/kb/935839>

MS08-032: Cumulative Security Update of ActiveX Kill Bits
<http://www.microsoft.com/technet/security/bulletin/MS08-032.mspx>

MS08-036: Vulnerabilities in Pragmatic General Multicast (PGM) Could Allow Denial of Service
<http://www.microsoft.com/technet/security/bulletin/MS08-036.mspx>

MS08-048: Security Update for Outlook Express and Windows Mail
<http://www.microsoft.com/technet/security/bulletin/MS08-048.mspx>

MS08-050: Vulnerability in Windows Messenger Could Allow Information Disclosure
<http://www.microsoft.com/technet/security/bulletin/MS08-050.mspx>

MS08-067: Vulnerability in Server Service Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx>

MS08-069: Vulnerabilities in Microsoft XML Core Services Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/MS08-069.mspx>

MS08-076: Vulnerabilities in Windows Media Components Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/MS08-076.mspx>

MS09-006: Vulnerabilities in Windows Kernel Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/MS09-006.mspx>

MS09-007: Vulnerability in SChannel Could Allow Spoofing
<http://www.microsoft.com/technet/security/bulletin/MS09-007.mspx>

MS09-010: Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/MS09-010.mspx>

MS09-011: Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution
<http://www.microsoft.com/technet/security/bulletin/MS09-011.mspx>

MS09-012: Vulnerabilities in Windows Could Allow Elevation of Privilege
<http://www.microsoft.com/technet/security/bulletin/MS09-012.mspx>

MS09-013: Vulnerabilities in Windows HTTP Services Could Allow Remote Code Execution

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

MS09-014: Cumulative Security Update for Internet Explorer

<http://www.microsoft.com/technet/security/bulletin/MS09-014.msp>

MS09-015: Blended Threat Vulnerability in SearchPath Could Allow Elevation of Privilege

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

5.0 Patch Installation Instructions and Customer Validation Form

Installing Patches



Note

Ensure the system has access to Microsoft's update web page before proceeding. If it does not have access, an alternative means of installing the patches must be arranged.

1. On the MIMS, log in to Windows as Administrator.

2. Installation procedures:

- a. Browse to <http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us>
- b. A pop-up may appear, click **Accept**.
- c. When the web site is displayed, click **Custom install**. The web site will now locate available patches for your system
- d. If a message is displayed stating, "We've made upgrades" click **Download** and proceed as described in step C.
- e. After the page has found the available patches, click **High-priority** on the left window.
- f. Ensure that Hologic has approved the selected patches before proceeding. Uncheck any patches that are not on the approval list.
- g. Click **Review and Install updates**.
- h. Click **Install Updates**. Select **Client install** and proceed to the next window.
- i. If windows appear prompting with questions, click **Accept**.
- j. After the patches have been downloaded, reboot the system.
- k. Log in and browse to **Control Panel > Add/Remove Programs**.
- l. Browse to the bottom of the list and ensure the patch you just downloaded is shown.



Note

If the system does not have direct access to Microsoft's update web page,

download the update from a separate PC or SUS server and place it on removable media.

System Testing

The objective of this section is to ensure patch installation did not compromise system stability. The user should complete the system regression tests outlined in this section successfully after the patches have been installed. If the following performance tests are inconclusive or fail, please contact Hologic Customer Service before placing the system in use.

1. Create a new V device

- a. From the service tools login, create a new device for future communication.
- b. Ensure the new V device can be communicated with via DICOM Echo.

2. Perform a DICOM Store

- a. From an external source (e.g. Selenia Acquisition Workstation) perform a DICOM Store request to MIMS.
- b. Verify the DICOM Store was successful.

3. Perform a DICOM Storage Commitment

- a. From an external source (e.g. Selenia Acquisition Workstation) perform a DICOM Storage Commitment request MIMS.
- b. Verify the DICOM Storage Commitment was successful.

3. Perform a Query/Retrieve

- a. Ensure the images can be retrieved from MIMS and viewed successfully on a workstation.

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 Hologic at 1.800.321.4659.