

Artwork consists of nine (10) 8 ½ inch x 11 inch sheet(s)

REV AUTHORED BY PETER LEWIS	DATE 06/19/06	 HOLOGIC [®] A FAMILY OF COMPANIES	Osteoporosis Assessment LORAD [®] Breast Cancer Detection DirectRay [®] Digital Imaging FLUOROSCAN [®] C-arm Imaging	 SIGNATURES ON FILE
REV DRAFTED BY PETER LEWIS	DATE 06/19/06			
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 QDR CYBERSECURITY PRODUCT REPORT	DOCUMENT NUMBER AW-01353	REV 004
REV. RELEASE DATE: 06/22/06	ARTWORK		SIZE A	SHEET 1 OF 1

QDR Cyber-Security Product Report

1.0 A Message To Our Customers

Hologic, Inc. continues its dedication and commitment to provide the highest quality products and services to help diagnose and treat your patients. We at Hologic are aware of the threat posed by malicious users and viruses. We would like to inform you of 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, Viruses and Malware

Hologic recognizes the need to react quickly to new attacks that may affect your systems. Of greatest concern to us are "Zero Day" exploits. These are attacks 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. This guide may be found at <http://www.hologic.com/cc/netwrksec.htm>
- Monitoring of recent vulnerabilities, including "proof of concept" testing.
Hologic's *Cyber Security Team* reviews and tests the recent exploits, assessing the potential for harm to Hologic products.
- Creation of a *Vulnerability Information Center* accessible via our website at <http://www.hologic.com/cc/netwrksec.htm>

2.0 Products Affected

This document pertains to the following product:

- QDR Systems running Windows XP

3.0 Anti-Virus

Hologic acknowledges your concern for obtaining virus protection. Therefore, we have evaluated QDR with anti-virus software. We have found the following anti-virus products to be compatible with QDR:

- Symantec Corporate Editions 9.0
- Symantec Corporate Editions 10.0
- McAfee 8.0i

Please contact your Hologic service representative for assistance with installation of these products. Instructions for installing and configuring these products can be found at Hologic's Cyber-Security Center: <http://www.hologic.com/cc/netwrksec.htm>

4.0 Operating System Updates and Security Patches

Hologic performs risk analysis to determine the potential consequences of published exploits. We also analyze any potential risk to the system created by applying a security patch. Because your QDR system is a registered medical device, Hologic must validate the effectiveness of recommended security patches. Only Hologic validated critical security patches should be installed on your QDR system. Service Packs must be tested and validated by Hologic and cannot be customer validated.

All System Updates and Security Patches to Windows XP as of June 14, 2006 have been validated to work with QDR.

List of validated System Updates and Security Patches:

- [Description of the critical update for Windows Firewall "My Network \(subnet\) only" scoping in Windows XP Service ...](#) 

This update helps narrow the definition of the "My network (subnet) only," or local subnet, restriction option in the Windows Firewall. ... any user intervention, use the following command: windowsxp-**kb886185**-x86-enu.exe /passive /quiet ... to restart, use the following command: windowsxp-**kb886185**-x86-enu.

- [Download details: Security Update for Windows Messenger \(KB887472\)](#) 

A security issue has been identified that could allow an attacker to compromise your Windows-based system and gain control over it. ... File Name: WindowsXP-**KB887472**-x86-enu.exe

- [MS04-041: A vulnerability in WordPad could allow code execution](#) 

This update resolves several newly discovered, privately reported vulnerabilities

- [MS04-043: Vulnerability in HyperTerminal could allow code execution](#) 

This update resolves a newly discovered, privately reported vulnerability. ... kbqfe kbsecurity kbwinnt400presp7fix kbsecbulletin kbwinxppresp2fix kbwin2000presp5fix kbwinserv2003presp1fix **KB873339** ...

- [MS04-044: Vulnerabilities in Windows Kernel and LSASS could allow elevation of privilege](#)

Resolves several newly discovered, privately reported vulnerabilities. ... kbqfe kbsecurity kbwinnt400presp7fix kbsecbulletin kbwinxppresp2fix kbwin2000presp5fix kbwinserv2003presp1fix **KB885835** ...

- [MS05-001: Vulnerability in HTML Help could allow code execution](#) 

This update resolves a newly discovered, publicly reported vulnerability. ... kbqfe kbsecurity kbwinnt400presp7fix kbsecbulletin kbwin2000presp5fix kbwinserv2003presp1fix kbwinxppresp3fix **KB890175** ...

- [Microsoft Security Bulletin MS05-004: ASP.NET Path Validation ...](#)

WindowsServer2003-**KB886903**-x86-ENU /passive /quiet To install the security update without forcing the system to restart, use the following command at a command prompt:

- [MS05-007: Vulnerability in Windows Could Allow Information Disclosure \(888302\)](#) 

Customers should install the update at the earliest opportunity. Bulletin is rated Important.

- [MS05-008: Vulnerability in Windows Shell Could Allow Remote Code Execution \(890047\)](#)



Customers should install the update at the earliest opportunity. Bulletin is rated Important

- [MS05_011: Vulnerability in server message block could allow remote code execution](#) 

Resolves a newly discovered, privately reported vulnerability. The vulnerability is documented in the "Vulnerability Details" section of the bulletin.

- [MS05-012: Vulnerability in OLE and COM Could Allow Remote Code Execution \(873333\)](#)



Customers should install the update at the earliest opportunity. Bulletin is rated Critical.

- [MS05-013: Vulnerability in the DHTML editing component ActiveX control could allow code execution](#) 

kbsecurity kbwinnt400presp7fix kbsecbulletin kbwinxppresp2fix kbwin2000presp5fix kbwinserv2003presp1fix
KB891781 ...

- [MS05-014: Cumulative security update for Internet Explorer](#) 


This update addresses the vulnerability discussed in Microsoft Security Bulletin MS05-014. To find out if other security updates are available for you, see the Overview section of this page

- [MS05-015: Vulnerability in hyperlink object library could allow remote code execution in Windows Server 2003](#) 

kbug kbfix kbsecvulnerability kbsecurity kbsecbulletin kbwin2000presp5fix kbwinserv2003presp1fix
KB888113. Article ...

- [MS05-018: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege and ...](#) 

This update resolves several newly-discovered, privately-reported vulnerabilities. Each vulnerability is documented in this bulletin in its own "Vulnerability Details" section of this bulletin. An attacker who successfully exploited the most ...

- [MS05-019: Vulnerabilities in TCP/IP could allow remote code execution and denial of service](#) 

This update resolves several newly discovered, privately reported, and public vulnerabilities. ... Remove button for the **KB893066** entry in the Add

- [MS05-026: Vulnerability in HTML Help Could ...](#)

This update resolves a newly-discovered, privately-reported vulnerability. A vulnerability exists in ... Microsoft Security Bulletin MS05-026 Vulnerability in HTML Help Could Allow Remote Code Execution ...

- [MS05-027: Vulnerability in Server Message Block Could Allow Remote Code Execution \(...\)](#) 

Administrators should also review the **KB896422**.log file for any failure messages when they use this ...

- [MS05-032: Vulnerability in Microsoft Agent Could Allow Spoofing \(890046\)](#) 

Administrators should also review the **KB890046**.log file for any failure messages when they use this ...

- [MS05-033: Vulnerability in Telnet Client Could Allow Information Disclosure \(896428\)](#) 

Administrators should also review the **KB896428**.log file for any failure messages when they use this ...

- [Microsoft Security Bulletin MS05-036: Vulnerability in Microsoft ...](#)


This update resolves a newly-discovered, privately-reported vulnerability. The vulnerability is documented in the "Vulnerability Details" section of this.....

- [MS05-040: Vulnerability in Telephony service could allow remote code execution](#) 

kbsecbulletin kbwinxppresp2fix kbpubtypekc kbwin2000presp5fix kbwinserv2003presp1fix kbmsccsearch **KB893756** ...

- [MS05-041: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service \(899591...\)](#) 

Administrators should also review the **KB899591**.log file for any failure messages when they use this ...

- [MS05-042: Vulnerabilities in Kerberos could allow denial of service, information disclosure, and spoofing](#) 

kbsecbulletin kbwinxppresp2fix kbpubtypekc kbwin2000presp5fix kbwinserv2003presp1fix kbmsccsearch **KB899587** ...

- [MS05-043: Vulnerability in Print Spooler service could allow remote code execution](#) 

kbsecbulletin kbwinxppresp2fix kbpubtypekc kbwin2000presp5fix kbwinserv2003presp1fix kbmsccsearch **KB896423** ...

- [MS05-045: Vulnerability in Network Connection Manager could allow ...](#)

Explains how to obtain security bulletin **MS05-045**. A denial of service vulnerability exists. An attacker who successfully exploited this vulnerability could cause components to stop responding.

- [MS05-046: Vulnerability in the Netware Client Could Allow Remote Code Execution \(899589\)](#) 

Administrators should also review the **KB899589**.log file for any failure messages when they use this ...

- [MS05-047: Vulnerability in Plug and Play Could Allow Remote Code Execution and Local ...](#) 

Administrators should also review the **KB905749**.log file for any failure messages when they use this

- [MS05-048: Vulnerability in the ...](#)

This update resolves a newly-discovered, privately-reported vulnerability that could allow an attacker to run arbitrary code on the system

- [MS05-049: Vulnerabilities in Windows Shell Could Allow Remote Code Execution \(900725\)](#) 

Administrators should also review the **KB900725**.log file for any failure messages when they use this ...

- [Microsoft Security Bulletin MS05-050: Vulnerability in DirectShow ...](#)

This update resolves a newly-discovered, privately-reported vulnerability. The vulnerability is documented in the "Vulnerability Details" section of this ...

- [MS05-051: Vulnerabilities in MSDTC and ...](#)

This update resolves several newly-discovered, privately-reported vulnerabilities. Each vulnerability is documented in this bulletin in its own ...

- [MS05-052: Cumulative security update for Internet Explorer](#) 

Describes the MS05-052 security update rollup for Internet Explorer. ... kbsecbulletin kbwinxppresp2fix kbpubtypekc kbwin2000presp5fix kbwinserv2003presp1fix kbmsccsearch **KB896688** ...

- [MS05-053: Vulnerabilities in graphics rendering engine could allow code execution](#) 

Describes how to obtain Microsoft Security Bulletin MS05-053.

- [MS05-054: Cumulative Security Update ...](#)

This update resolves several newly-discovered, publicly and privately reported vulnerabilities. Each vulnerability is documented in its own Vulnerability ...

- [MS06-001: Vulnerability in graphics rendering engine could allow ...](#)

Discusses how to obtain Microsoft security bulletin **MS06-001**: Vulnerability in graphics rendering engine could allow remote code execution.

- [MS06-002: Vulnerability in embedded Web fonts could allow remote code ...](#)

Discusses how to obtain Microsoft Security Bulletin **MS06-002**: Vulnerability in embedded Web fonts could allow remote code execution.

- [MS06-004: Cumulative security update for Internet Explorer](#)

Describes the **MS06-004** security update rollup for Internet Explorer.

- [MS06-005: Vulnerability in Windows Media Player could allow remote ...](#)

Describes the **MS06-005** security bulletin for Windows Media Player. The associated security update fixes a vulnerability in Windows Media Player that could allow remote code execution.

- [MS06-006: Vulnerability in Windows Media Player plug-in with non ...](#)

Describes the **MS06-006** security bulletin for Windows Media Player that discusses the vulnerability that could allow remote code execution in non-Microsoft Internet browsers.

- [MS06-007: Vulnerability in TCP/IP could allow denial of service](#)

Describes the **MS06-007** security bulletin for TCP/IP that discusses the vulnerability that could allow a denial of service.

- [MS06-008: Vulnerability in WebClient could allow remote code execution](#)

Describes the **MS06-008** security bulletin. The associated security update fixes a vulnerability in WebClient that could allow remote code execution.

- [MS06-013: Cumulative security update for Internet Explorer](#)

This update resolves several newly-discovered, publicly and privately reported vulnerabilities. ... Microsoft Security Bulletin MS06-013 Cumulative Security Update for Internet Explorer (912812)

- [MS06-014: Vulnerability in Microsoft Data Access Components \(MDAC ...](#)

Windowsserver2003-**kb911562**-x86-enu /quiet Note Use of the /quiet switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to ...

- [MS06-015: Vulnerability in Windows Explorer Could Lead to Remote Code ...](#)

Windowsserver2003-**kb908531**-x86-enu /quiet Note Use of the /quiet switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to ...

- [MS06-016: Cumulative Security Update for Outlook Express](#)

Windowsserver2003-**kb911567**-x86-enu /quiet Note Use of the /quiet switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to ...

- [Malicious Software Removal Tool](#)

The free Microsoft Malicious Software Removal Tool scans your hard disk for and tries to remove ... Malicious Software Removal Tool Published: January 11, 2005 | Updated: April 11, 2006

- [Microsoft Security Bulletin MS06-018: Vulnerability in Microsoft ...](#)

This update resolves several newly discovered, privately reported vulnerabilities. Each vulnerability is documented in this bulletin in its own ...

- [MS06-021: Cumulative Update for Internet Explorer 6 SP1 ...](#)

File Name: IE6.0sp1-**KB916281**-Windows-2000-XP-x86-ENU.exe: Version: 916281: Security Bulletins: MS06-021: Knowledge Base (KB) Articles: **KB916281**: Date Published: 6/7/2006

- [MS06-022: Vulnerability in ART Image Rendering Could Allow ...](#)

Vulnerability in ART Image Rendering Could Allow Remote Code Execution in Internet Explorer 6 Service Pack 1 (**KB918439**) Brief Description

- [MS06-023: JScript 5.1 Security Update for Windows 2000 SP4 ...](#)

JScript 5.1 Security Update for Windows 2000 SP4 (**KB917344**) Brief Description

- [MS06-024: Security Update for Windows Media Player 10 for ...](#)

Security Update for Windows Media Player 10 for Windows XP (**KB917734**) Brief Description

- [MS06-025: Vulnerability in Routing and ...](#)

Windowsserver2003- **kb911280**-x86-enu /quiet. Note Use of the /quiet switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to ...

- [Microsoft Security Bulletin MS06-027: Vulnerability in Microsoft Word ...](#)

Microsoft Works Suite 2002 - Download the update (**KB917335**) (same as the Microsoft Word 2002 update) • Microsoft Works Suite 2003 - Download the update (**KB917335**) (same as the Microsoft Word 2002 ...

- [MS06-030: Vulnerability in Server Message ...](#)

Windowsserver2003- **kb914389**-x86-enu /quiet. Note Use of the /quiet switch will suppress all messages. This includes suppressing failure messages.

- [MS06-032: Vulnerability in TCP/IP Could ...](#)

Windowsserver2003-kb917953-x86-enu /quiet. Note Use of the /quiet switch will suppress all messages. This includes suppressing failure messages. Administrators should use one of the supported methods to ...

- [Windows Malicious Software Removal Tool](#)

... you would like to run this tool more than once a month, run the version that is available from this Web page or use the version on the Malicious Software Removal Tool Web site. Please review **KB890830** ...

- [Description of the Windows Genuine Advantage Notifications application ...](#)

This article describes the Microsoft Windows Genuine Advantage Notifications application. ...
Keywords: B : kbsecurity kbexpertiseinter kbhowto **KB905474**

5.0 Installing Patches



Note Ensure the system has access to Microsoft's update webpage before proceeding

1. On the QDR computer, login to Windows as an Administrator.
2. Installation procedures:
 - a. Exit QDR without shutdown.
 - b. Browse to <http://update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us>
 - c. A pop-up may appear. If so, click "ACCEPT from Microsoft".
 - d. When the website is displayed, click "**Custom install.**" The website will now locate available patches for your system.
 - e. If a message is displayed saying "We've made upgrades" click "**Download**" and proceed as described in step c.
 - f. After the page has found the available patches, click **High-priority** on the left window.
 - g. Ensure that the patches that are selected have been approved by Hologic before proceeding. Uncheck any patches that are not on the approval list.
 - h. Click "**Review and Install**" updates.
 - i. Click "**Install Updates.**" Select "**Client install**" and proceed to the next window.
 - j. If windows appear prompting with questions, click "**Accept.**"
 - k. After the patches have been downloaded, reboot the system.
 - l. Log in as an Administrator and browse to Control panel > Add/Remove Programs
 - m. 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 webpage, download the update from a separate PC or SUS server and place it on removable media.

Questions and Concerns

If you have any questions or concerns, please contact Hologic Customer Service at 800.321.4659.