

InSight 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:

- InSight Systems running Windows XP

3.0 Anti-Virus

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

- Symantec Corporate Edition 10.0
- McAfee 8.0i

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 InSight 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 InSight 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 13, 2007 have been validated to work with InSight.

List of validated System Updates and Security Patches:

- [Security Update for Windows XP \(KB896423\)](#)
- [Windows Malicious Software Removal Tool – November 2006 \(KB890830\)](#)
- [MS06-068: Security Update for Windows XP \(KB920213\)](#)
- [MS06-066: Vulnerability in the Client Service could allow remote code execution \(KB923980\)](#)
- [MS06-070: Vulnerability in Workstation Service could allow remote code execution \(KB924270\)](#)
- [MS06-069: Vulnerabilities in Macromedia Flash Player from Adobe could allow remote code execution \(KB923789\)](#)
- [MS06-067: Cumulative security update for Internet Explorer \(KB922760\)](#)

- [MS06-071: Security update for Microsoft XML Core Services 4.0 \(KB927978\)](#)
- [MS06-063: Vulnerability in Server Service could allow denial of service \(KB923414\)](#)
- [MS06-065: Vulnerability in Windows Object Packager could allow remote execution \(KB924496\)](#)
- [MS06-057: Vulnerability in Windows Explorer could allow remote code execution \(KB923191\)](#)
- [MS06-061: Vulnerabilities in Microsoft XML Core Services could allow remote code execution \(KB924191\)](#)
- [MS06-064: Vulnerabilities in TCP/IP IPv6 could allow denial of service \(KB922819\)](#)
- [MS06-055: Vulnerability in Vector Markup Language could allow remote code execution \(KB925486\)](#)
- [Update for Windows XP \(KB922582\)](#)
- [Update for Windows XP \(KB916595\)](#)
- [MS06-052 Security Update for Windows XP \(KB919007\)](#)
- [MS06-053: Vulnerability in Indexing Service could allow cross-site scripting\(KB920685\)](#)
- [Update for Windows XP \(KB920872\)](#)
- [MS06-051: Vulnerability in the Windows kernel could result in remote execution \(KB917422\)](#)
- [MS06-050: Vulnerabilities in Microsoft Windows Hyperlink Object Library could allow remote code execution \(KB920670\)](#)
- [MS06-041: Vulnerability in DNS resolution could allow remote code execution \(KB920683\).](#)
- [MS06-045: Vulnerability in Windows Explorer could allow remote code execution \(KB921398\).](#)
- [MS06-046: Vulnerability in HTML Help could allow remote code execution \(KB922616\)](#)

- [MS06-043: Vulnerability in Microsoft Windows could allow remote code execution \(KB920214\)](#)
- [MS06-036: A vulnerability in the DHCP Client Service could allow remote code execution \(KB914388\)](#)
- [MS06-025: Vulnerability in Routing and Remote Access could allow remote code execution \(KB911280\)](#)
- [MS06-024: Vulnerability in Windows Media Player could allow remote code execution \(KB917734\)](#)
- [MS06-030: Vulnerability in Server Message Block could allow elevation of privilege \(KB914389\)](#)
- [MS06-023: Vulnerability in Microsoft JScript could allow remote code execution \(KB917344\)](#)
- [MS06-022: Vulnerability in ART image rendering could allow remote code execution \(KB918439\)](#)
- [MS06-018: Vulnerability in Microsoft Distributed Transaction Coordinate could allow denial of service \(KB913580\)](#)
- [MS06-032: Vulnerability in TCP/IP could allow remote code execution \(KB917953\)](#)
- [Update for Windows XP \(KB900485\)](#)
- [MS06-015: Vulnerability in Windows Explorer could lead to remote code \(KB908531\)](#)
- [MS06-016: Cumulative Security Update for Outlook Express \(KB911567\)](#)
- [MS06-014: Vulnerability in Microsoft Data Access Components \(MDAC\) function could allow code execution \(KB911562\)](#)

- [MS06-008: Vulnerability in WebClient could allow remote code execution \(KB911927\)](#)
- [MS06-006: Vulnerability in Windows Media Player plug-in with non-Microsoft internet browsers could allow remote code execution \(KB911564\)](#)
- [MS06-002: Vulnerability in embedded Web fonts could allow remote code execution \(KB908519\)](#)
- [MS06-001: Vulnerability in graphics rendering engine could allow remote code execution \(KB912919\)](#)
- [Update for Windows XP \(KB910437\)](#)
- [MS05-050: Vulnerability in DirectShow could allow remote code execution \(K904706\)](#)
- [Microsoft Security Bulletin MS05-053: Vulnerabilities in graphics rendering engine code allow code execution \(KB896424\)](#)
- [MS05-047: Vulnerability in Plug and Play could allow remote code execution \(KB905749\)](#)
- [MS05-049: Vulnerabilities in the Windows shell could allow for remote code execution \(KB900725\)](#)

- [MS05-051: Vulnerabilities in MS DTC and COM+ could allow remote code execution \(KB902400\)](#)
- [Security Update for Windows XP \(KB901017\)](#)
- [MS05-045: Vulnerability in Network Connection Manager could allow denial of service \(KB905414\)](#)
- [MS05-040: Vulnerability in Telephony service could allow remote code execution \(KB893756\)](#)
- [MS05-041: Vulnerability in Remote Desktop Protocol could allow denial of service \(KB899591\)](#)
- [MS05-042: Vulnerabilities in Kerberos could allow denial of service \(KB899587\)](#)
- [Update for Windows XP \(KB894391\)](#)
- [MS05-026: A vulnerability in HTML Help could allow remote code execution \(KB896358\)](#)
- [MS05-018: Vulnerabilities in Windows kernel could allow elevation of privilege and denial of service \(KB890859\)](#)
- [MS05-036: Vulnerability in Microsoft Color Management Module could allow remote code execution \(KB901214\)](#)
- [MS05-033: Vulnerability in Telnet client could allow information disclosure \(KB896428\)](#)
- [MS04-044: Vulnerabilities in Windows Kernel and LSASS could allow elevation of privilege \(KB885835\)](#)
- [MS05-007: Vulnerability in Windows could allow information disclosure \(KB888302\)](#)

- [MS05-009 Security Update for Windows Messenger \(KB887472\)](#)
- [MS05-013: Vulnerability in the DHTML editing component ActiveX control \(KB891781\)](#)
- [MS04-043: Vulnerability in HyperTerminal could allow code execution \(KB873339\)](#)
- [Critical Update for Windows XP \(KB886185\)](#)
- [MS04-041: A vulnerability in WordPad could allow code execution \(KB885836\)](#)
- [MS06-061: Security update for Microsoft XML Core Services 4.0 SP2 KB925672\)](#)
- [Cumulative Security Update for Internet Explorer for Win XP – KB925454](#)
- [MS06-075: Vulnerability in Windows could allow elevation of privilege - KB926255](#)
- [Cumulative Security Update for Outlook Express for Win XP – KB923694](#)
- [MS06-078: Vulnerability in Windows Media Format could allow remote code execution – KB925398](#)
- [MS06-078: Vulnerability in Windows Media Format could allow remote code execution – KB923689](#)
- [Windows malicious software removal tool – December 2006 – KB890830](#)
- [MS07-006: Vulnerability in Windows Shell could allow elevation of privilege \(KB928255\)](#)
- [MS07-008: A vulnerability in the HTML Help ActiveX control could allow remote code execution \(KB928843\)](#)
- [MS07-007: Vulnerability in Windows Image Acquisition Service could allow elevation of privilege \(KB927802\)](#)
- [MS07-012: Vulnerability in Microsoft Foundation Classes could allow for remote code execution \(KB924667\)](#)

- MS07-009: Vulnerability in Microsoft Data Access Components could allow remote code execution (KB927779)
- MS07-013: Vulnerability in Microsoft RichEdit could allow remote code execution(KB918118)
- MS07-011: Vulnerability in Microsoft OLE Dialog could allow remote code execution (KB926436)
- MS07-016: Cumulative security update for Internet Explorer (KB928090)
- February 2007 cumulative time zone update for Microsoft Windows operating systems (KB931836)
- Microsoft Windows Malicious Software Removal Tool (KB890830)
- MS07-004: Vulnerability in Vector Markup Language could allow remote code execution (KB929969)
- MS07-027 - addresses a vulnerability in Microsoft Windows (KB931768)
- MS07-017 - Vulnerabilities in GDI Could Allow Remote Code Execution (KB925902)
- MS07-019: Vulnerability in UPnP could allow remote code execution (KB931261)
- MS07-020: Vulnerability in Microsoft Agent could allow remote code execution (KB932168)
- MS07-021: Vulnerability in Windows CSRSS could allow remote code execution (KB930178)
- MS07-022: Vulnerability in the Windows kernel could allow elevation of privilege (KB931784)

5.0 Installing Patches



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

1. On the InSight computer, login to Windows as an Administrator.
2. Installation procedures:
 - a. Exit InSight without shutdown.
 - b. Browse to <http://update.microsoft.com/windowsupdate/v6/default.aspx?In=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 selected are 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.