Medical Device Security
Health Group
Digital Output

Security Assessment
Report for the *Kodak* Color Medical Imager 1000 (CMI-1000) Software Version 1.1

Part Number 1G0434
Revision 2.0
June 21, 2005

Table of Contents

Executive Summary

Kodak Health Group ("Kodak") has recognized that digital imaging and related patient data requires an overall approach to include privacy & security requirements in the product design stage. In addition, mitigation processes are required to significantly increase system security and patient safety. This document consists of a summary of the *Kodak* Color Medical Imager 1000 (CMI-1000) software v1.1 (hereafter referred to as the "Product") security assessment, mitigation processes, and actions taken by Kodak to assist the medical community.

Testing procedures entailed analyzing the device for security vulnerabilities using vulnerability scanners, assessing the configuration for National Security Agency (NSA) Hardening Guidelines, and analyzing HIPAA Capabilities. Direct assessment procedures used at Kodak are able to verify implementation of HIPAA security controls.

Extensive steps have been taken to harden the *Windows* Operating System and to authenticate all types of users. The *Windows* XP Embedded Operating System is secured above and beyond the default configuration in all required services, accounts, and ports so that a standard malware that assumes a default configuration will fail. *Windows* XP Embedded user account policies, user rights, and security options were configured to satisfy relevant NSA guidelines.

Health Group Overview

The worldwide trend of migrating images & patient data from film to an electronic format is rapidly reaching many aspects of the medical community. One of the areas affected is the medical imaging sector, where patient-identifiable information can be found in an electronic format in a variety of computer systems, many of which are medical devices. Since these devices contain patient information, they need to be hardened to protect confidentiality. Additionally, the FDA monitors medical device manufactures to ensure the hardware and software functionality meets diagnostic and patient safety requirements.

Kodak has assigned a Malware Quick Action Team (MQAT) and a Network Vulnerability Protection (NVP) Lab to assess the current state of security of a medical device and to assist customers with protection of such devices. These teams focus is on protecting the confidentiality of patient-identifiable information, ensuring data integrity, and protecting the functionality of a medical device.

After the assessment, Kodak works with both OS vendors and medical facilities to deploy updates as required that mitigate vulnerabilities. In many cases the medical facility can increase security through network design, such as using virtual local area networks (VLANs) and firewalls. If this process occurs prior to installation, security can be built into the network infrastructure, saving significant time and future effort. In conjunction with network infrastructure security, Kodak provides service modifications that include

OS and application configuration changes that incorporate OS vendor patches to increase security. Limitations in this area are that any changes made to a medical device must fit into the change management plan that the FDA has approved for this device.

Product Description

The Product is a PC-based color medical printing system that runs the *Windows* XP Embedded Operating System. The Product is operated by using a touch screen local panel, thus, not requiring the use of the keyboard/mouse by the normal user.

The custom user interface limits the user to the specific functions defined for the product; hence, preventing user access to the operating system's desktop. Medical Images and DICOM IOD's are the only files that are transmitted and received over the TCP/IP network using the DICOM protocol. No EMAIL services are configured or available to the user.

Extensive steps have been taken to harden the *Windows* OS and to authenticate all types of users. The *Windows* XP Embedded Operating System is secured above and beyond the default configuration in all required services, accounts, and ports so that a standard malware that assumes a default configuration will fail. *Windows* XP Embedded user account policies, user rights, and security options were configured to satisfy relevant NSA guidelines.

Field Service users require identification and authorization through a mechanism closely controlled by Kodak. This helps ensure that product configuration is controlled and those with access to it are properly trained.

Assessment Methodology

Assessments consist of three areas; vulnerability assessment, hardening guidelines comparison, and HIPAA control analyses. The vulnerability assessment portion is conducted by using a commercially available security scanner. The scanner electronically probes the device for security holes that may allow a hacker or malware to compromise a system. Vulnerabilities identified range in severity, depending upon the degree of possible damage and likelihood that an attack could occur. For example a vulnerability that allows malware to crash Internet Explorer would be less severe than a vulnerability that would allow a hacker to alter information on the hard drive.

During the hardening guideline comparison, device configurations are analyzed and compared to the NSA Hardening Guidelines. For the HIPAA enabling functionality, critical areas are examined. This provided verification that items such as password protection are being implemented. All aspects of the assessment are documented in technical reports and can be provided to the medical community.

Process Methodology

The MQAT and NVP processes are designed to assist medical device users to increase security of current devices and to build security into future releases. This is accomplished through a multi-tier assessment process that provides the medical community with information on how to increase security of a device. The process includes an evaluation of the vulnerabilities, system configuration and HIPAA controls. If weaknesses in the device security are identified, mitigation steps are developed from this assessment and the OS provider and Kodak work to reduce vulnerabilities. After mitigation, a second assessment is completed to document any changes that influenced security of the device.

Tested security updates of *Microsoft* patches for the Product are made available for the installed base after the Malware Quick Action Team has confirmed that the Product is vulnerable to the security threat.

Conclusion

The Product was assessed at the Kodak development lab in Plano, TX. Testing procedures entailed analyzing the device for security vulnerabilities using security assessment tools (STAT, NMAP, NESSUS) and NSA Hardening Guidelines, as well as HIPAA security requirements. The results of the scans of the system identified the TCP & UDP network ports active, in addition which security patches were implemented for this device. A port scan of the system identified 5 open ports, none of which are typically open by malware.

Kodak's testing included the capability of our medical customers for active user authentication controls related to the HIPAA security rule. These mainly fall under the "Technical Controls" area. Details of the Hardening and OS compliance and the security patches that reduce impact of known vulnerabilities are included at the end of this report.

Results

User Authentication:

- Users must log on to the product (not the OS) with a username and password at the user interface prior to accessing PHI-related information (user authentication).
- User passwords and all user management related fields are stored in an encrypted form when exported to the Product's configuration diskette.
- Service Users must authenticate by means of a time-sensitive based digital certificate issued by Kodak prior to allowing access to the system administration tool (AccessLink).
- All Service access occurs through a secure encrypted tunnel between the Service Users' PC and the product (SecureLink).
- Access to the Product desktop requires an active connection to a service laptop that has exchanged a Kodak digital certificate with the Product, and then a subsequent logon to an OS user account. (SecureDesktop).
- The number of OS user accounts is limited. Guest account is disabled and the Administrator account is renamed.
- OS logon screen does not display the last logged on user.
- OS accounts do not use a portion of the username as the password.
- SQL Server database logon requires *Microsoft Windows* credentials or SQL Server credentials locally or via the network.
- New software including binaries (.exe or .dll files) and scripts (.vbs or .bat) can only be installed on the Product by an authorized Kodak Service Technician running with a current authentication certificate.

Operating System & Operating System Components:

- Latest Service Pack is installed for the *Windows* XP Embedded Operating System (SP2).
- No automatic update components are enabled on the product.
- *Microsoft* Outlook Express is un-installed. There is no e-mail transfer or user agent on the system, and the SMTP and IMAP ports are blocked, so the system is invulnerable to viruses that propagate via e-mail.
- Public community rights for the SNMP Service are removed.
- Operating System Services that are not required by the Product are configured to start manually or disabled as appropriate.
- All TCP network ports are closed with the exception of these ports:
  443 - HTTPS

445	- Service Access
5040	- DICOM Communications
8091	- Application Access

- All UDP network ports are filtered by IP Address with the exception of these ports (required for the Product software to run):

445	- Service Access

- Latest *Microsoft* Security patches are installed at the time the official production release media is generated (see security patches).
- The Kodak software release process ensures that any software release or system image must undergo a full virus scan with latest virus definitions before release to the field.

Security Patches Included in CMI-1000 v1.1:

1. MS05-019 Vulnerabilities in TCP/IP Could Allow Remote Code Execution and Denial of Service (893066)
2. MS05-011 Vulnerability in Server Message Block Could Allow Remote Code Execution (885250)
3. MS03-031 SQL Server 2000 (32-bit) Security Patch (KB867460)
4. XP Embedded SP2 (includes MS05-007, MS05-008, MS05-011, MS05-012, MS05-013, MS05-014, and MS05-015)
5. MS05-001 XP Embedded SP2 QFE: *Microsoft* Security Bulletin (890175)
6. December, 2004 *Microsoft* Security Bulletins MS04-038 (834707), MS04-041 (885836), MS04-043 (873339), and MS04-044 (885835)