Medical Device Security
Health Imaging
Digital Capture

Security Assessment
Report for the Kodak Capture Link Server V1.00

Version 1.0

Table of Contents

Table of Contents……2

Executive Summary……3

Overview ……3

Product Description…….4

Assessment Methodology……..4

Process Methodology……..5

Conclusion.…….5

Results…....…….6

Executive Summary

Kodak Health Imaging ("Kodak") has recognized that digital imaging and related patient data require 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 Capture Link Server V1.00 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 OS and to authenticate all types of users. The Windows 2000 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 2000 user account policies, user rights, and security options were configured to satisfy relevant NSA guidelines (see references).

Health Imaging 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 Process (NVP) to assess the current state of security of a medical device and to assist customers with protection of such devices. These team's foci are 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 approved for the device.

Product Description

The DirectView Capture Link Server V1.00 system consists of a standalone PC that runs the Windows 2000 Operating System. This system is operated by the normal user through the use of a keyboard and mouse.

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. Only web pages, database commands and proprietary communication protocols are transmitted and received by this product over the TCP/IP network. No EMAIL services are configured or available to the customer.

Extensive steps have been taken to harden the Windows OS and to authenticate all types of users. The Windows 2000 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 2000 user account policies, user rights, and security options were configured to satisfy relevant NSA guidelines (see references).

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 four commercially available security scanners. Each 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 allow malware to crash Internet Explorer would be less severe that a vulnerability that would allow a hacker to alter information on a hard drive.

Scanners are used to reduce false positives that may occur when only one scanner is used. Additionally, scanners vary widely in vulnerability detection since their probing techniques are different. 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 provides 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 in increasing 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.

Conclusion

The Capture Link Server software V1.00 was assessed at the Kodak development lab in Rochester, NY. Testing procedures entailed analyzing the device for security vulnerabilities using security assessment tools (STAT, NMAP, NESSUS), NSA Hardening Guidelines, and HIPAA security requirements. The results of the scans of the system identified the TCP & UPD network ports active, and which security patches were implemented on this device. A port scan of the system identified twenty-one open ports, none of which are typically open by malware.

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

Results

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

User Authentication:

- Users must logon to the product (not the OS) with a username and password at the user interface prior to accessing PHI related information (user authentication).
- Service Users must authenticate by means of a time sensitive 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).
- Capture Link software runs without a user logged on to an OS account.
- Access to the Capture Link desktop requires an active connection to a service laptop that has exchanged a Kodak digital certificate with the Capture Link System, and then a subsequent logon to an OS user account. (SecureDesktop).
- Number of OS user accounts are limited. Guest account is disabled.
- OS accounts do not use a portion of the username as the password.
- PCAnyWhere (Version 10.5) is configured for local access only and the network port for PCAnyWhere is closed.
- SQL Server database logon requires MS Windows credentials or SQL Server credentials locally or via the network.

Operating System & Operating System Components:

- Latest Service Pack is installed for the Windows 2000 operating system (SP4).
- No automatic update components are enabled on the product.
- Microsoft Outlook Express is un-installed.
- Public community rights for the SNMP Service are removed.
- Operating System Services that are not required by the DirectView Software are configured to start manually or disabled as appropriate.
- All TCP network ports are closed with the exception of these ports:
  80 – IIS – HTTP
  135 – RPC
  139 – Drive Sharing

190 – DCOM
210 – DirectView Service Access
220 – DirectView Service Access
443 – HTTPS (secure tunnel)
623 – Security Listener
1433 – SQL
2761 – DCOM
2762 – DCOM
4190 – DirectView Application
4191 – DirectView Application
5000-5020 - SQL DTC
5040 – DICOM PrintSCP
5041 – PACS Push Connection
12207 – DirectView Application
14626 – DirectView Application
58431 – RIG/RDET

Ports 80, 135, 139, and 1443 are filtered by IP Address based on the system configuration of connected systems.

- All UDP network ports are filtered by IP Address with the exception of these ports (required for the DirectView software to run):
  123 – NTP
  137 – NetBIOS
  138 – NetBIOS

- Latest Microsoft Security patches are installed at the time the official trade trial release media is generated (see security patches).

References:

1. Windows 2000 Security Checklist – LabMice.Net
2. Guide to Securing Microsoft Windows 2000 File and Disk Resources – NSA
3. Guide to Securing Microsoft Windows 2000 Group Policy – NSA
4. Guide to Securing Microsoft Windows 2000 Active Directory – NSA
5. Guide to Securing Microsoft Windows 2000 DHCP – NSA
6. Guide to Securing Microsoft Windows 2000 Encrypting File System – NSA
   Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set – NSA

Security Updates Released for DirectView Capture Link Server V1.00 Software:

1. Security Update 02-05-01

Security Patches Included in DirectView Capture Link Server V1.00:

1. Microsoft Windows 2000 Service Pack 4 (327194)

2. MS04-014: Vulnerability in the Microsoft Jet Database Engine could permit code execution (837001)
3. MS04-012: Cumulative Update for Microsoft RPC/DCOM (828741)
4. MS04-011: Security Update for Microsoft Windows (835732)
5. MS04-007: An ASN.1 vulnerability could allow code execution (828028)
6. MS03-049: Buffer Overrun in the Workstation Service Could Allow Code Execution (828749)
7. MS03-045: Buffer overrun in the ListBox and in the ComboBox Control could allow code execution (824141)
8. MS03-044: Buffer Overrun in Windows Help and Support Center Could Lead to System Compromise (825119)
9. MS03-043: Buffer Overrun in Messenger Service Could Allow Code Execution (828035)
10. MS03-042: Buffer Overflow in Windows Troubleshooter ActiveX Control Could Allow Code Execution (826232)
11. MS03-041: Vulnerability in Authenticode Verification Could Allow Remote Code Execution (823182)
12. MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146)
13. MS03-034: Flaw in NetBIOS Could Lead to Information Disclosure (824105)
14. MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980)
15. MS03-023: Buffer Overrun In HTML Converter Could Allow Code Execution (823559)
16. MS03-011: Security Update Microsoft Virtual Machine (Microsoft VM) (816093)
17. MS02-050 Certificate Validation Flaw Could Enable Identity Spoofing (Q329115).
18. Recommended Update for Windows 2000 (822831)
19. L2TP/IPSec NAT-T Update for Windows XP and Windows 2000 (818043)
20. Jet 4.0 Service Pack 8 (829558)
21. Computer stops responding (hangs) when it tries to mount an NTFS volume after you restart the computer (820888)
22. MS04-030: Vulnerability in WebDAV XML message handler could lead to a denial of service (824151)
23. MS04-038: Cumulative Security Update for Internet Explorer (834707)
24. MS04-024: A vulnerability in the Windows shell could allow remote code execution (839645)
25. MS04-023: Vulnerability in HTML Help could allow code execution (840315)
26. MS04-032: Security update for Microsoft Windows (840987)
27. MS04-037: Vulnerability in Windows shell could allow remote code execution (841356)
28. MS04-031: Vulnerability in NetDDE could allow remote code execution (841533)
29. MS04-020: A vulnerability in POSIX could allow code execution (841872)

30. MS04-022: A vulnerability in Task Scheduler could allow code execution (841873)
31. MS04-019: A vulnerability in Utility Manager could allow code execution (842526)
32. How to disable the ADODB.Stream object from Internet Explorer (870669)
33. (147222)
34. MS02-008: XMLHTTP control in MSXML 4.0 can allow access to local files (317244)
35. MS02-008: XMLHTTP Control in MSXML 2.6 Can Allow Access to Local Files (318202)
36. MS02-008: XMLHTTP Control in MSXML 3.0 Can Allow Access to Local Files (318203)
37. SQL Server 2000 SP3 Updates to MDAC 2.7 SP1 (328797)
38. MS02-040: Security Update for Microsoft Data Access Components (823718)
39. Update for Windows Media Player URL script command behavior (828026)
40. MS04-003: Buffer overrun in an MDAC function could allow code execution (832483)
41. .NET Framework 1.1 Service Pack 1 (SP1) (867460)
42. MS02-032: Windows Media Player Rollup Available (320920)