Medical Device Security
Health Imaging
Digital Capture

Security Assessment
Report for the Kodak DryView 8150 Imager Release 1.0

Table of Contents

Executive Summary

Kodak Health Imaging ("Kodak") recognizes 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 DryView 8150 Imager Release 1 security assessment, mitigation processes, and actions taken by Kodak to assist the medical community after product installation.

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 Kodak configuration of the Windows 2000 Operating System provides greater security beyond the default configuration so that only the required services, accounts, and ports are active, reducing the risks of the majority of malware released to date. 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 and hardcopy 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 (or PHI – patient health information) is in 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 increase security and patient confidentiality. Additionally, medical device manufactures are required to comply with FDA regulations 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 qualified updates as required that mitigate vulnerabilities. In addition it is vital that medical facility include network security through network design concepts, such as using virtual local area networks (VLANs), application filtering and departmental firewalls. The result should increase medical device performance increase application and network security, reduce vulnerability risks, save significant time and future patching effort. .

Note, the only limitation is to provide qualified patches to any medical device and must follow the quality process specified by FDA regulations for all medical devices.

Product Description

The DryView 8150 imager contains an embedded PC that runs the Windows 2000 Operating System. The imager is operated by using a touch screen; 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 on Windows 2000 Service Pack 4. The Kodak configuration of the Windows 2000 Operating System provides greater security beyond the default configuration so that only the required services, accounts, and ports are active, reducing the risks of the majority of malware released to date. . 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 a commercially available security scanner. The scanner electronically probes the device for security holes that may allow a hacker or malware 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.

During the hardening guideline comparison, device configuration were analyzed and compared to the NSA Hardening Guidelines. For the HIPAA enabling functionality, critical areas were examined. This verified that items such as password protection are being implemented in this release. 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 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.

Conclusion

The DryView 8150 Imager Release 1 was assessed at the Kodak development lab in Plano, TX. Testing procedures entailed analyzing the device for security vulnerabilities using for security assessment tools (STAT, NMAP, NESSUS) using NSA Hardening Guidelines, as well as, HIPAA security requirements. The results of the scans of the system identified the TCP & UPD network ports active, in addition which security patches were implemented for this device. A port scan of the system identified seventeen 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 which include security patches to reduce impact of know vulnerabilities are included at the end of this report.

Results

Tested security updates of Microsoft patches for the DryView 8150 Imager was made available for the installed base on 5/12/2004. NVP lab performed security assessment on 9/21/2004.

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).
- User passwords and all user management related fields are stored in an encrypted form when exported to the DryView 8150 Imager's configuration diskette.
- 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).
- Access to the DryView 8150 Imager desktop requires an active connection to a service laptop that has exchanged a Kodak digital certificate with the DryView 8150 Imager, and then a subsequent logon to an OS user account. (SecureDesktop).
- Number of OS user accounts are 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 MS 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 a DV8150 system 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 2000 operating system (SP4).
- 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 Simple Mail Transfer Protocol (SMTP) and Internet

Message Access Protocol (IMAP) ports are blocked, so the system is invulnerable to viruses that propagate via e-mail.

- Public community rights for the Simple Network Management Protocol (SNMP) Service are removed.
- Operating System Services that are not required by the DryView 8150 Imager are configured to start manually or disabled as appropriate.
- All TCP network ports are closed with the exception of these ports:
  21 - ftp
  53 - DNS2
  80 - http
  85 - IIS
  190 - Service Access
  191 - Service Access
  443 - HTTPS
  1433 - SQL
  2243 - SQL
  2433 - SQL
  4096 - MIS
  4097 - SimMCSServer
  5040 - DICOM print SCP
  5631 - PCAnywhere

- All UDP network ports are filtered by IP Address with the exception of these ports (required for the DirectView software to run):
  53 - DNS
  67 - DHCP
  68 - DHCP
  1433 - SQL
  5632 - PCAnywhere

- 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.

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

7. Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set – NSA

Security Patches Included in the DryView 8150 Imager Release 1:

1. MS00-055 Scriptlet Rendering Vulnerability (Q269368).
2. MS00-093 Browser Print Template and File Upload via Form Vulnerabilities (Q279328).
3. MS02-042 Flaw in Network Connection Manager Could Enable Privilege Elevation (Q326886).
4. MS02-045 Unchecked Buffer in Network Share Provider can lead to Denial of Service (Q326830).
5. MS02-048 Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172).
6. MS02-050 Certificate Validation Flaw Could Enable Identity Spoofing (Q329115).
7. MS02-055 Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255).
8. MS02-063 Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks (Q329834).
9. MS02-069 Flaw in Microsoft VM Could Enable System Compromise (***810030***).
10. MS02-070 Flaw in SMB Signing Could Enable Group Policy to be Modified (Q329170).
11. MS02-071 Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation (Q328310).
12. MS03-001 Unchecked Buffer in Locator Service Could Lead to Code Execution (Q810833).
13. MS02-064 Windows 2000 Default Permissions Could Allow Trojan Horse Program (Q327522).
14. MS02-065 Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414).
15. MS03-026 Blaster Worm: Critical Security Patch for Windows 2000
16. MS02-062 Cumulative Patch for Internet Information Service (Q327696).
17. Microsoft Internet Explorer 6 Service Pack 1 (Windows 2000)*
18. Cumulative Security Update for Internet Explorer 6 SP1 (KB824145)
19. 330994: April 2003, Security Update for Outlook Express 6 SP1
20. Security Update for Microsoft Windows (KB828749)
21. Q329115: Security Update (Windows 2000)
22. Security Update for Microsoft Windows 2000 (KB828035)
23. Security Update for Microsoft Windows 2000 (KB825119)
24. Security Update for Microsoft Windows 2000 (KB826232)
25. Security Update for Microsoft Windows 2000 (KB824105)
26. Security Update for Microsoft Windows 2000 (KB823182)
27. Security Update for Microsoft Windows 2000 (KB824141)
28. Security Update for Microsoft Windows 2000 (KB824146)

29. 823559: Security Update for Microsoft Windows 2000
30. 816093: Security Microsoft Virtual Machine (Microsoft VM)
31. Update for Windows Media Player Script Commands (KB828026)
32. Security Update for Microsoft Data Access Components (823718)
33. 814078: Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP)
34. Security Update, February 13, 2002 (MSXML 2.6)
35. Cumulative Security Update for Outlook Express 6 Service Pack 1 (KB837009)
36. Cumulative Security Update for Internet Explorer 6 Service Pack 1 (KB832894)
37. Security Update for Windows 2000 (KB828741)
38. Security Update for Windows 2000 (KB835732)
39. Security Update for Windows 2000 (KB837001)