Security and Malware Prevention Steps
Kodak DryView 8900 Laser Imager v2.1

Last Updated 7/2/04

The DryView 8900 Laser Imager functions as a DICOM SCP and can accept print jobs from DICOM modalities. The DryView 8900 runs the Windows 2000 Operating System as an embedded application on a PC enclosure without a keyboard, monitor, or mouse connected.

The only user interface for the product is the local panel on the front of the imager that is physically connected to the PC (no common access to the desktop). The local panel limits the user to the specific functions defined for the product. 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 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.

Tested security updates of Microsoft patches for the DryView 8900 are made available for the installed base after the Malware Quick Action Team has confirmed that the DryView 8900 is vulnerable to the security threat (see security updates).

User Authentication:

- Users must logon to the product (not the OS) with a username and password at the local panel 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 8900 backup configuration set.

- 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).

- 8900 software runs with a user logged on to a restricted OS account with restricted desktop settings.

- Access to the 8900 desktop requires an active connection to a service laptop that has exchanged a Kodak digital certificate with the 8900, 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.

- Secure OS user accounts by restricting them to explicit areas of the registry and file system.

- SQL Server database logon requires MS Windows credentials or SQL Server credentials locally or via the network.

- Users cannot initiate software updates of any kind to the product. AutoRun is disabled for CD-ROM drive.

Operating System & Operating System Components:

- WebServer (IIS) is locked down using a standard utility provided by Microsoft.

- 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.

- All TCP network ports are closed with the exception of these ports:
  21 – FTP
  53 – DNS
  80 – HTTP
  85 – IIS
  190 – Service Access
  191 – Service Access
  210 – Service Access
  443 – HTTPS (secure tunnel)
  1433 – SQL
  2243 – SQL
  2433 – SQL
  4096 – SDS
  4097 – SimMCSServer
  5040 – DICOM PrintSCP
  5199 – MIM Service Access
  5631 – pcAnywhere

- All UDP network ports are closed with the exception of these ports (required for the MIM software to run):
  53 – DNS
  67 – DHCP
  68 – DHCP
  1433 – SQL
  5632 – pcAnywhere

- Anti-virus software is run against the master image used for creating the production release media.

- Latest Microsoft Security patches are installed at the time the official production 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 Group Policy: Security Configuration Tool Set – NSA

Security Patches Included in 8900 v2.1:

Windows Security Updates 8900 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).

Windows Security Updates Added for 8900 Release 2

1. Microsoft Internet Explorer 6 Service Pack 1 (Windows 2000)
2. MS03-048 Cumulative Security Update for Internet Explorer 6 SP1 (KB824145)
3. MS03-014 April 2003, Security Update for Outlook Express 6 SP1 (330994)
4. MS03-049 Security Update for Microsoft Windows (KB828749)
5. MS02-050 Security Update for Microsoft Windows 2000(KB329115)
6. MS03-043 Security Update for Microsoft Windows 2000 (KB828035)
7. MS03-044 Security Update for Microsoft Windows 2000 (KB825119)
8. MS03-042 Security Update for Microsoft Windows 2000 (KB826232)
9. MS03-034 Security Update for Microsoft Windows 2000 (KB824105)
10. MS03-041 Security Update for Microsoft Windows 2000 (KB823182)
11. MS03-045 Security Update for Microsoft Windows 2000 (KB824141)
12. MS03-039 Security Update for Microsoft Windows 2000 (KB824146)
13. MS03-023 Security Update for Microsoft Windows 2000 (823559)
14. MS03-011 Security Microsoft Virtual Machine (Microsoft VM) (816093)
15. Update for Windows Media Player Script Commands (KB828026)
16. MS03-033 Security Update for Microsoft Data Access Components (823718)
17. Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP) (814078)
18. Security Update, February 13, 2002 (MSXML 2.6)