Security and Malware Prevention Steps
Kodak DirectView CR Version 3.x.x
Kodak DirectView CR Version 2.2.1
Kodak DirectView DR Version 1.x.x
Last Updated 6/03/2004

The DirectView Computed Radiography (CR) and Digital Radiography (DR) systems contain an embedded PC that runs the Windows 2000 Operating System. Older versions (CR 2.2.1, and DR 1.0.5) operate on a PC that runs the Windows NT Operating System. Most of the CR systems are operated by using a touch screen; thus, not requiring the use of the keyboard/mouse by the user. The DR systems and the CR 500 system provide a mouse and keyboard for additional interaction 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.

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 CR and DR Systems are made available for the installed base after the Malware Quick Action Team has confirmed that the CR and DR Systems are vulnerable to the security threat (see security updates).

User Authentication:

- CR/DR software runs without a user logged on to an OS account.
- Access to the CR/DR desktop requires access to the Kodak Service account.
- Numbers of OS user accounts are limited.
- OS accounts do not use a portion of the username as the password.
- PCAnyWhere (Version 10.0) 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 (SP3 or SP4 depending on release date).
- Latest Service Pack is installed for the Windows NT operating system (SP6a).
- 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.

- 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 Encrypting File System – NSA
   Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set – NSA

Security Updates Released for DirectView CR V3.x.x Software:

1. Digital Capture Mod Kits

Security Patches Included in DirectView CR V3.x.x Software:

1. Microsoft Windows 2000 Service Pack 3
1. MS03-024: Buffer Overrun in Windows Could Lead to Data Corruption (Q817606)
2. MS03-028: Heap Overrun in HTR Chunked Encoding Might Enable Web Server Compromise
3. A Lock Occurs Between Two Threads of System GDI in Windows 2000 (Q322842)
4. MS02-048 Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172).
5. MS02-055 Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255).
6. MS02-053: Request to SmartHTML Interpreter May Monopolize Web Server CPU Resources (Q324096)
7. MS02-051: Cryptographic Flaw in RDP Protocol Can Cause Information Disclosure
8. MS02-045 Unchecked Buffer in Network Share Provider can lead to Denial of Service (Q326830).
9. MS02-042 Flaw in Network Connection Manager Could Enable Privilege Elevation (Q326886).

Security Updates Released for DirectView CR V2.2.1 Software:

1. Digital Capture Mod Kits

Security Patches Included in DirectView CR V2.2.1:

1. Microsoft Windows NT 4.0 Service Pack 6a
2. Microsoft Post-Windows NT 4.0 Service Pack 6a Security Rollup Package (Q299444).

Security Updates Released for DirectView DR V1.0.5 Software:

1. Digital Capture Mod Kits

Security Patches Included in DirectView DR V1.0.5:

1. Microsoft Windows NT 4.0 Service Pack 6a
2. Microsoft Post-Windows NT 4.0 Service Pack 6a Security Rollup Package (Q299444)?
3. MS03-026: Buffer Overrun In RPC Interface Could Allow Code Execution (823980)
4. MS03-039: Buffer Overrun In RPCSS Service Could Allow Code Execution (824146)

5. MS03-001 Unchecked Buffer in Locator Service Could Lead to Code Execution (Q810833).
6. MS02-006: An Unchecked Buffer in the SNMP Service May Allow Code to Run
7. MS00-006: Index Server Error Message Reveals Physical Location of Web Folders

Security Updates Released for DirectView DR V1.1.x Software:

1. Digital Capture Mod Kits

Security Patches Included in DirectView DR V1.1.x:

1. Microsoft Windows 2000 Service Pack 3
2. MS02-055: Unchecked Buffer in Windows Help Facility Could Enable Code Execution (Q323255).
3. MS02-048: Flaw in Certificate Enrollment Control Could Allow Deletion of Digital Certificates (Q323172).
4. MS02-042: Flaw in Network Connection Manager Could Enable Privilege Elevation (Q326886).
5. MS02-071: Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation (Q328310).
6. MS02-045: Unchecked Buffer in Network Share Provider can lead to Denial of Service (Q326830).
7. MS02-050: Certificate Validation Flaw Could Enable Identity Spoofing (Q329115).
8. MS02-051: Cryptographic Flaw in RDP Protocol Can Cause Information Disclosure
9. MS02-053: Request to SmartHTML Interpreter May Monopolize Web Server CPU Resources (Q324096)
10. MS02-070: Flaw in SMB Signing Could Enable Group Policy to be Modified (Q329170).
11. MS02-063: Unchecked Buffer in PPTP Implementation Could Enable Denial of Service Attacks (Q329834).
12. MS03-001: Unchecked Buffer in Locator Service Could Lead to Code Execution (Q810833).
13. MS03-007: Unchecked Buffer in Windows Component May Cause Web Server Compromise (Q815021)
14. MS03-010: Flaw in RPC endpoint mapper could allow Denial of Service attacks
15. MS02-069: Flaw in Microsoft VM Could Enable System Compromise - Eight Vulnerabilities. (Q810030)
16. Q811630: Windows 2000 Patch: Enabling Applications to Access HTML Help in a New, Restricted Mode
17. MS02-065: Buffer Overrun in Microsoft Data Access Components Could Lead to Code Execution (Q329414)