SECURITY BULLETIN

Kodak PACS Product Security Bulletin - Blaster Worm

Eastman Kodak Company's Health Imaging Group is committed to providing products and services that can help you treat your patients with "A Better View of Life." We are aware of the recent attacks through the Internet, including the one sometimes referred to as the LovSan/MSBlast or Blaster Worm, and of the problems this malicious software (malware) may have caused to your networks and the computers connected to them, including your Kodak products. We are also aware of additional vulnerabilities recently announced by Microsoft to computers using one of several versions of their Windows operating system. Kodak wants you to know what we are doing to help you deal with these active and potential malware issues.

The worm and its variants are also known as W32.Blaster.Worm, W32.Blaster.C.Worm, W32.Blaster.B.Worm, W32.Randex.E (Symantec), W32/Lovsan.worm (McAfee), WORM_MSBLAST.A (Trendmicro), and Win32.Posa.Worm (Computer Associates). Commonly known as "Blaster," this worm exploits the vulnerability that was addressed by Microsoft Security Bulletin MS03-026 (Update #823980) to spread itself over networks by using open Remote Procedure Call (RPC) ports on computers that are running any of the following products:

Microsoft Windows XP Professional
Microsoft Windows XP Home Edition
Microsoft Windows XP Media Center Edition
Microsoft Windows XP Tablet PC Edition
Microsoft Windows Server 2003, Web Edition
Microsoft Windows Server 2003, Standard Edition
Microsoft Windows Server 2003, Enterprise Edition
Microsoft Windows Server 2003, Datacenter Edition
Microsoft Windows 2000 Server
Microsoft Windows 2000 Professional
Microsoft Windows 2000 Datacenter Server
Microsoft Windows 2000 Advanced Server
Microsoft Windows NT Server
Microsoft Windows NT Advanced Server
Microsoft Windows NT Server, Enterprise Edition
Microsoft Windows NT Workstation 4.0
Microsoft Windows NT Server 4.0 Terminal Server Edition
Microsoft Windows XP 64-Bit Edition Version 2002
Microsoft Windows XP 64-Bit Edition Version 2003
Microsoft Windows Server 2003, 64-Bit Enterprise Edition

Symptoms of Infection

Some customers whose computers have been infected may not notice the presence of the worm at all, while others who are not infected may experience problems because the worm is attempting to attack their computer. Typical symptoms may include Windows XP and Windows Server 2003 systems rebooting every few minutes without user input, or Windows NT 4.0 and Windows 2000 systems becoming unresponsive.

If your computer is infected with this worm, you may not experience any symptoms, or you may experience any of the following symptoms:

- You may receive the following error messages:

The Remote Procedure Call (RPC) service terminated unexpectedly.
The system is shutting down. Please save all work in progress and log off.
Any unsaved changes will be lost.
This shutdown was initiated by NT AUTHORITY\SYSTEM.

- The computer may shut down, or may restart repeatedly, at random intervals.
- On a Windows XP-based or on a Windows Server 2003-based computer, a dialog box may appear that gives you the option to report the problem to Microsoft. After you submit the error report, the following Microsoft Web page may be shown on your computer:

  http://oca.microsoft.com/en/response.asp?sid=699

- If you are using Windows 2000 or Windows NT, you may receive a "Stop" error message on a blue screen.
- You may find a file that is named Msblast.exe, Nstask32.exe, Penis32.exe, Teekids.exe, Winlogin.exe, Win32sockdrv.dll, or Yuetyutr.dll in the Windows\System32 folder.
- You may find unusual TFTP* files on your computer.

Actions Being Taken

Kodak has been in contact with Microsoft to obtain their recommended repairs and patches to the computer operating systems in our products that might be vulnerable to this malware. Kodak has been working to qualify the patches and hotfixes supplied by our vendors for installation. As you are aware, (and unlike PCs used exclusively for word processing or at home for example), our imagers, digital output, PACS Link, and PACS systems are developed and maintained in strict accordance with FDA regulations to ensure their clinical utility and to protect patient safety. Accordingly, our risk analysis process requires that we ensure the fixes offered by our suppliers work without causing any impact to image quality or functional performance, before we release them for installation into systems in the field. This careful process of checking patches in the laboratory has already discovered incompatibilities in the “Blaster” fixes from Microsoft, resulting in the need for us to make modifications that were then included in Kodak's approved release. Without these changes, untested system patches to existing installations could have resulted in undesirable consequences.

Kodak has issued a Service Bulletin to its Field Service organization regarding the “Blaster” worm that details the recommended actions, including the installation and verification procedures for the Service Pack and Security Update that are appropriate for the products detailed below. Customers should contact their Kodak Service Representative for assistance in installing service packs and security updates. Customers also have the option, and may choose to install the Service Pack and Security Update on their own, but do so AT THEIR OWN RISK. Kodak has detailed the necessary procedures that customers choosing to perform the installations themselves MUST follow. Ignoring the documented procedures may result in extended downtime, performance degradation, increased service costs and may place patient data at risk. Customers who wish to acquire these procedures should contact their Kodak Service Representatives. Repairs made by Kodak Service personnel that are a direct result of customer installation of the Service Pack and Security Update will be charged on a time and material basis.

Kodak PACS Product Implications

To guard against unauthorized access of Kodak servers and workstations, Kodak has performed a limited validation of Microsoft's Windows Service Packs and the "Blaster" worm Security Update (#823980). Based on experiences reported from the field and the validation process, the following recommendations are being made to the Kodak products potentially affected by the "Blaster" worm:

ClinicalAccess 4.1 client workstations: Customers still running this version are strongly encouraged to upgrade to DirectView TX 4.2 and DirectView CX/DX version 4.2/4.3 if it also exists on the system. The application of Service Packs and Security Updates is the responsibility of the customer/user and is AT THEIR OWN RISK. Kodak Service is not responsible for these systems.

DirectView TX 4.2 client workstations on Windows NT: No successful attacks of Windows NT – based PACS systems have been reported to Kodak, although the vulnerability exists according to Microsoft. Kodak has qualified Service Pack 6a and Microsoft Security Update #823980. The application of Service Packs and Security Updates is the responsibility of the customer/user and is AT THEIR OWN RISK. Kodak Service is not responsible for these systems.

DirectView TX 4.2 client workstations on Windows 2000: Kodak is recommending the installation of Windows Security Update #823980, which is available from Microsoft. (Note, the installation of Windows Security Update #823980 expects that Service Pack 4 has been previously installed.) The application of Service Packs and Security Updates is the responsibility of the customer/user and is AT THEIR OWN RISK. Kodak Service is not responsible for these systems.

DirectView *DirectView Web Distribution System 4.5 / PACS System 5.x web client workstations*: The application of Service Packs and Security Updates is the responsibility of the customer/user and is AT THEIR OWN RISK. Kodak Service is not responsible for these systems.

AccuRad 4.0.x/4.1.x on Windows NT: Customers still running this version are strongly encouraged to upgrade to DirectView CX/DX version 4.2/4.3 and DirectView TX 4.2 if present on the system. *HP LC3 Netservers running Windows NT may experience degraded performance after upgrading to DirectView CX/DX* 4.2*.*

ClinicalAccess Server 4.1.x on Windows NT: Customers still running this version are strongly encouraged to upgrade to DirectView TX 4.2 and DirectView CX/DX version 4.2 / 4.3 if it also exists on the system. *HP LC3 Netservers running Windows NT may experience degraded performance after upgrading to DirectView* TX 4.2*.*

DirectView CX/DX 4.2.x on Windows NT: No successful attacks of Windows NT – based PACS systems have been reported to Kodak, although the vulnerability exists according to Microsoft. Kodak has qualified Service Pack 6a and Microsoft Security Update #823980. Customers should contact their Kodak Service Representative for assistance in installing these service packs and security updates. Customers who choose to apply Service Pack 6a and Security Update #823980 themselves do so AT THEIR OWN RISK.

DirectView TX Server 4.2 on Windows NT: No successful attacks of Windows NT – based PACS systems have been reported to Kodak, although the vulnerability exists according to Microsoft. Kodak has qualified Service Pack 6a and Microsoft Security Update #823980. Customers should contact their Kodak Service Representative for assistance in installing these service packs and security updates. Customers who choose to apply Service Pack 6a and Security Update #823980 themselves do so AT THEIR OWN RISK.

SECURITY BULLETIN

DirectView CX/DX 4.2.x/4.3.x on Windows 2000: Kodak is recommending the installation of Windows Security Update #823980, which is available from Microsoft. Customers should contact their Kodak Service Representative for assistance in installing these service packs and security updates. Customers who choose to install this update themselves do so AT THEIR OWN RISK. (Note, the installation of Windows Security Update #823980 expects that Service Pack 4 has been previously installed.)

> Note: DirectView CX/DX 4.3.x systems with Dictaphone Powerscribe integration should only be upgraded to Windows 2000 Service Pack 3 as it is the highest level supported by Powerscribe at this time. Kodak is recommending that all customers with Dictaphone Powerscribe integration contact Kodak Service for assistance.

DirectView TX Server 4.2 on Windows 2000: Kodak is recommending the installation of Windows Security Update #823980, which is available from Microsoft. Customers should contact their Kodak Service Representative for assistance in installing these service packs and security updates. Customers who choose to install this update themselves do so at their own risk. (Note, the installation of Windows Security Update #823980 expects that Service Pack 4 has been previously installed.)