KODAK HEALTH IMAGING SECURITY BULLETIN

Kodak Healthcare Information Systems (PACS & RIS) Product Security Bulletin –Microsoft MS04-018 through MS04-024 Security Bulletins

Kodak Products Affected by MS04-022, MS04-023, MS04-024:

System 4 PACS Display
System 5 PACS Display (Microsoft Windows based)
RIS 2010
RIS v7

July 2004 Vulnerabilities Reported By Microsoft.

Microsoft has released seven (7) security bulletins for July 2004, which include MS04-018 through MS04-024, affecting customers using Microsoft Internet Explorer and CD Direct, components of Microsoft Windows; Windows XP, Windows 2000, Windows Server 2003, Windows Millennium Edition, Windows 98, and Windows 98 Second Edition. Kodak has completed a risk analysis for all vulnerabilities and identified that ***only*** MS04-022; MS04-023 and MS04-024 could create a critical risk to Kodak's PACS System 4 and System 5, RIS 2010, and RIS v7. Kodak recommends that authorized Kodak service agents or customers immediately download and install the following Microsoft updates.

Kodak Product	Operating System	Vulnerability	Update Name	Version
PACS System 4 & 5, RIS 2010, RIS v7	Windows 2000	MS04-023	Windows2000-KB840315-x86-ENU.EXE	840315
PACS System 4 & 5, RIS 2010, RIS v7	Windows 2000	MS04-022	Windows2000-KB841873-x86-ENU.EXE	841873
PACS System 4 & 5, RIS 2010, RIS v7	Windows 2000	MS04-024	Windows2000-KB839645-x86-ENU.EXE	839645

Customers should contact their Kodak Service Representative for assistance in the installation of the patches for the Microsoft Windows; Internet Explorer, Windows XP, Server 2003 and 2000 operating systems. The recommended downloads identified in the table above. The Kodak Service organization will provide support for customers who choose to request assistance for these products. This will include the appropriate downloads, installation and operating verification for the products involved.

Customers also have the option of choosing to download, install and verify operational performance for the products involved on their own, but do so at their own risk. Microsoft has detailed the necessary procedures for customers choosing to perform these changes themselves, and recommend you should contact your System Administrator. Disregarding the documented procedures may result in extended downtime, performance degradation, increased service costs, and may place patient data at risk of compromise of its integrity or of its confidentiality. Repairs completed by Kodak Service personnel that are a direct result of customer installation of this security update will be charged on a time and material basis.

Note: Kodak has validated all updates for MS04-018 through MS04-024 to reduce potential future risks for the vulnerabilities identified. Our customers should acknowledge that the Kodak PACS System 4 and System 5, RIS 2010, and RIS v7 have low risk to the vulnerabilities identified for MS04-018 through MS04-021**.**

Kodak Healthcare Information Systems Product Implications

Kodak's Network Vulnerability Protection lab has performed analysis on the July 2004 Microsoft Security Bulletins, the identified vulnerabilities and risks are as follows:

Vulnerability	Severity Rating*	Impact of Vulnerability	Risk to Kodak Products
MS04-024	Moderate	Remote code execution vulnerability exists in the Windows Shell	Attacker who successfully exploits this vulnerability *could* take control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges *only* when an administrative user is logged on.
MS04-023	Critical	Two remote code execution vulnerability exists in the in HTML Help	Attacker who successfully exploits this vulnerability *could* take control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges *only* when an administrative user is logged on.
MS04-022	Critical	Remote Code Execution vulnerability exists in the Task Scheduler	Attacker who successfully exploits this vulnerability *could* gain the clinical user same privileges.
MS04-021	Low	Buffer overrun vulnerability in Internet Information Server 4.0	No known impact to Kodak products.
MS04-020	Low	Remote Code Execution vulnerability exists in the POSIX	Attacker *could* exploit this vulnerability, if they have a valid logon to gain system control to run a malicious program.
MS04-019	Low	Remote Code Execution vulnerability exists in the Utility Manager	Attacker *could* successfully exploit this vulnerability if they have valid logon credentials and are local
MS04-018	Low	Denial of service vulnerability that allows attacker to send specially designed e-mail messages	No known impact to Kodak products.