KODAK HEALTH IMAGING SECURITY BULLETIN

Kodak Healthcare Information Systems (PACS & RIS) Product Security Bulletin –Microsoft MS04-027, MS04-028 Security Bulletins

Kodak Products Affected by MS04-027*, MS04-028

System 4 PACS Display, Software Version 4.3.2, 4.2.2.1
System 5 PACS Display, Software Version 5.0, 5.1
RIS 2010 Web
VIParchive Web Client
Archive Server Web UI
CD Direct, Software Version 3.0, 3.5

*** Kodak Products Affected by MS04-027**

Vulnerability only exploits Kodak systems that have Office 2000, Word Perfect 5.x Converter installed

September 17, 2004 Vulnerabilities Reported By Microsoft.

Microsoft has released a security bulletins on September 15, 2004, for MS04-027 and MS04-028, affecting customers using Microsoft Internet Explorer 6.0 SP1 components running on Operating Systems Windows 2000 and XP. Kodak has completed a risk analysis and is active in the validation of the security updates for this vulnerability. This validation includes the Kodak's PACS System 4 and System 5, CD Direct, RIS 2010 Web, Archive Server Web UI and VIParchive Web Client with Internet Explorer installed. **Kodak recommends that customers do not use the diagnostic and/or clinical workstations to access un-trusted web sites. Additionally, Kodak recommends users to login to Windows via conventional user accounts that do not have any administrative privileges (e.g., not in the Administrators group).**

Kodak Product	Microsoft Component	Vulnerability	Update Name	Version
PACS System 4 and 5, RIS 2010	Office 2000: WordPerfect 5.x Converter	MS04-027	office2000-kb873380-fullfile-enu.exe	1
PACS System 4 and 5, RIS 2010 Web, Archive Server Web UI, VIParchive Web Client, CD Direct	Internet Explorer 6 SP1	MS04-028	IE6.0sp1-KB833989-x86-ENU.exe	6

Upon the completion of Kodak's validation of these security updates, the results will be posted on the Kodak web site. Customers should subsequently contact their Kodak Service Representative for assistance in the installation. Kodak recommends that customers only install the recommended downloads identified in the table above once they have been validated. 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 only the updates identified above for MS04-27 and MS04-028 to reduce potential future risks for the vulnerabilities identified. Our customers should acknowledge that the Kodak PACS System 4 and System 5, CD Direct, RIS 2010 Web, Archive Server Web UI and VIParchive Web Client should be configured to access to only trusted web sites and use only conventional user accounts in order to reduce the security risk associated with the vulnerabilities identified above**.**

Kodak Healthcare Information Systems Product Implications

Kodak's Network Vulnerability Protection Lab has completed the risk analysis on the MS04-027 and MS04-028 Microsoft Security Bulletins, the identified vulnerabilities and risks are as follows:

Vulnerability	Severity Rating	Impact of Vulnerability	Risk to Kodak Products
MS04-027	Important	Remote code execution vulnerability exists in the Microsoft WordPerfect 5.*x* Converter.	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.
MS04-028	Critical	Buffer overrun and remote code execution vulnerability exists in the Internet Explorer 6.0 SP1	a) Exploitation of buffer overrun vulnerability in the processing of JPEG Image formats in web pages. **Note: No risks related to JPEG compression of DICOM images.** b) 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.