KODAK HEALTH IMAGING SECURITY BULLETIN

Kodak Healthcare Information Systems (PACS & RIS) Product Security Bulletin –Microsoft MS04-029 - MS04-038 Security Bulletins

Kodak Products Affected by Critical Vulnerability Level: MS04-032, MS04-034, MS04-037 And MS04-038

System 4 PACS Display, Software Version 4.3.2, 4.2.2.1
System 5 PACS Display, Software Version 5.0, 5.1, 5.1.1
RIS 2010 Client, RIS 2010 Web
VIParchive Web Client
Archive Server Web UI
CD Direct, Software Version 3.0, 3.5

Kodak Products Affected by Important Vulnerability Level: MS04-029, MS04-030 And MS04-031

System 4 PACS Display, Software Version 4.3.2, 4.2.2.1
System 5 PACS Display, Software Version 5.0, 5.1, 5.1.1
RIS 2010 Client, RIS 2010 Web
VIParchive Web Client
Archive Server Web UI
CD Direct, Software Version 3.0, 3.5

Kodak Products Not Affected by Vulnerabilities: MS04-033, MS04-035, And MS04-036

Kodak products do not utilize: Excel 2000, 2002, Microsoft Exchange Server 2003, Windows XP 64-Bit Edition Version 2003, or Windows Server 2003, or Windows NNTP component

---

October 12, 2004 Vulnerabilities Reported By Microsoft.

Microsoft has released ten (10) security bulletins on October 12, 2004, for MS04-029 through MS04-038, affecting customers using a large variety (see table below) of Microsoft products and services. Kodak has completed a risk analysis for all vulnerabilities and identified that *only* MS04-032; MS04-034; MS04-037 and MS04-038 could create a *critical* risk to Kodak's PACS System 4 and System 5, RIS 2010 Web, Archive Server Web UI or VIParchive Web Client.

Kodak has completed the validation of these *critical* security updates; customers should install these *critical* security updates as described below.

Kodak Product	Microsoft Component	Vulnerability	Update Name	Version
PACS System 4 and 5, RIS 2010 Web, Archive Server Web UI, VIParchive Web Client	a) Win NT 4.0 SP6a b) Win 2000 SP3 c) Win XP SP1	MS04-032	a) WindowsNT4Server-KB840987-x86-ENU.exe b) Windows2000-KB840987-x86-ENU.EXE c) WindowsXP-KB840987-x86-enu.exe	840987
PACS System 4 and 5, RIS 2010 Web, Archive Server Web UI, VIParchive Web Client	Win XP SP1	MS04-034	WindowsXP-KB873376-x86-enu.exe	873376

KODAK HEALTH IMAGING SECURITY BULLETIN

Kodak Product	Microsoft Component	Vulnerability	Update Name	Version
PACS System 4 and 5, RIS 2010 Web, Archive Server Web UI, VIParchive Web Client	a) Win NT 4.0 SP6a b) Win 2000 SP3 c) Win XP SP1	MS04-037	a) WindowsNT4Server-KB841356-x86-ENU.exe b) Windows2000-KB841356-x86-ENU.EXE c) WindowsXP-KB841356-x86-enu.exe	841356
PACS System 4 and 5, RIS 2010 Web, Archive Server Web UI, VIParchive Web Client	IE 6.0 SP1 on: a) Win NT 4.0 SP6a b) Win 2000 SP3 c) Win XP SP1	MS04-038	a) IE6.0sp1-KB834707-Windows-NT4sp6a-98-ME-x86-ENU.exe b) IE6.0sp1-KB834707-Windows-2000-XP-x86-ENU.exe c) IE6.0sp1-KB834707-WindowsXP-ia64-ENU.exe	834707

Kodak has completed validation of these security updates; 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 will validate only the critical security updates identified above. For security updates MS04-029, MS04-30 and MS04-031, our customers must acknowledge that they should actively upgrade their systems, according to the table below, to reduce the security risk identified by Microsoft.

Vulnerability	Severity Rating	Impact of Vulnerability	Risk to Kodak Products	Upgrade Recommendation
MS04-029	Important	Information disclosure and denial of service attacks associated with Win NT 4.0 SP6a	Attacker who successfully exploits this vulnerability *could* stop the system from responding or potentially read portions of active memory content. **End of Microsoft support for Win NT 4.0 is Dec. 31, 2004,**	Upgrade System 4 on Win NT 4.0 to System 5.1.1

KODAK HEALTH IMAGING SECURITY BULLETIN

Vulnerability	Severity Rating	Impact of Vulnerability	Risk to Kodak Products	Upgrade Recommendation
MS04-030	Important	Denial of Service	Attacker who successfully exploits this vulnerability *could* stop the system from responding	a) Upgrade System 4 on Win 2000 to System 5.1.1 b) Upgrade System 5.x on Win XP SP1 to Win XP SP2
MS04-031	Important	Remote code execution vulnerability exists in the NetDDE services	An attacker who successfully exploited this vulnerability *could* take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. Note: the NetDDE services are not started by default and would have to be manually started, or started by an application that requires NetDDE, for an attacker to attempt to remotely exploit this vulnerability.	a) Upgrade System 4 on Win NT 4.0 to System 5.1.1 b) Upgrade System 5.x on Win XP SP1 to Win XP SP2

Complete Listing of Risks to Kodak Healthcare Information Systems

Kodak's Network Vulnerability Protection Lab has completed the risk analysis on the MS04-029 through MS04-038 Microsoft Security Bulletins, the identified vulnerabilities and risks are as follows:

Vulnerability	Severity Rating	Impact of Vulnerability	Risk to Kodak Products
MS04-029	Important	Information disclosure and denial of service	An attacker *could* exploit this vulnerability of information disclosure through the ability to read portions of active memory content or create a denial of service that could cause the affected system to stop responding
MS04-030	Important	Denial of Service through WebDAV	An attacker *could* exploit this vulnerability and could cause WebDAV to consume all available memory and CPU time on an affected server

KODAK HEALTH IMAGING SECURITY BULLETIN

Vulnerability	Severity Rating	Impact of Vulnerability	Risk to Kodak Products
MS04-031	Important	Remote code execution vulnerability exists in the NetDDE services	Attacker An attacker *could* exploit this vulnerability and take complete control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full privileges. **Note:** the NetDDE services would have to be manually started, or started by an application that requires NetDDE, for an attacker to attempt to remotely exploit.
MS04-032	Critical	Remote code execution	An attacker *could* exploit this vulnerability and take control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts that have full administrative rights, or complete a denial of service attack.
MS04-033	Critical	Remote code execution through Excel	No known impact to Kodak products.
MS04-034	Critical	Remote Code Execution vulnerability exists in the Windows processes Compressed (zipped) folders	An attacker *could* exploit this vulnerability and take control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges, user interaction is required.
MS04-035	Critical	Remote Code Execution vulnerability exists in the Windows SMTP component	No known impact to Kodak products.
MS04-036	Critical	Remote Code Execution vulnerability exists in the Windows NNTP component	No known impact to Kodak products.
MS04-037	Critical	Remote Code Execution vulnerability exists in the Windows Shell	An attacker *could* exploit this vulnerability and take control of an affected system, including installing programs; viewing, changing, or deleting data; or creating new accounts with full privileges

Vulnerability	Severity Rating	Impact of Vulnerability	Risk to Kodak Products
MS04-038	Critical	Five remote code execution and three information disclosure vulnerabilities exist in Internet Explorer. Critical Risks: a) Cascading Style Sheets (CSS) Heap Memory Corruption Vulnerability b) Similar Method Name Redirection Cross Domain Vulnerability c) Install Engine Vulnerability	An attacker *could* exploit this vulnerability and 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.