KODAK HEALTH IMAGING SECURITY BULLETIN

Kodak Digital Output Systems (DryView & MIM, 9410) Product Security Bulletin –Microsoft MS04-029 - MS04-038 Security Bulletins

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

DryView Systems, 8900, 8150
MIM Systems, Software Version 3.2.1, 4, 5, 5.0.1, 5.2, 6.0, 6.1
9410 System

Kodak Products Not Affected by Critical Vulnerability Level: MS04-032, MS04-034, MS04-036, MS04-037 And MS04-038

Kodak Digital Capture products do not utilize the Microsoft software and components identified in the October Security Bulletins.

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

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

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*** MS04-029; MS04-030 and MS04-031 could create an ***important*** risk to Kodak's DryView 8900, 8150, MIM SW v 3.2.1, 4, 5, 5.0.1, 5.2, 6.0, 6.1 and 9410.

For MS04-030 a specially crafted remote WebDAV message(s) would have to be generated through a unauthorized established Web session, applications at the greatest risk are e-commerce applications. For MS04-031 an unauthorized user would have to gain access and manually start NetDDE services to attempt to remotely exploit this vulnerability. In normal operations the Digital Output products do not use these functionalities. Kodak will include the MS04-030 and MS04-031 security updates in the next software release. Systems that use the Win NT operating system should be upgraded to the current Digital Output systems.

Kodak Product	Microsoft Component	Vulnerability	Update Name	Version
MIM Systems SW v 3.2.1, 4, 5, 5.0.1, 5.2 9410 System	a) Win NT 4.0 SP6a **Note: effects products running on Win NT 4.0**	MS04-029	a) WindowsNT4Server-KB873350-x86-ENU.exe **Note: End of Microsoft support for Win NT 4.0 is Dec. 31, 2004,**	873350
MIM Systems SW v 6.0, 6.1 DryView 8900, 8150 9410 System	Win 2000 SP3; components WebDAV, IIS	MS04-030	Windows2000-KB824151-x86-ENU.EXE	824151
MIM Systems SW v 3.2.1, 4, 5, 5.0.1, 5.2, 6.0, 6.1 DryView 8900, 8150 9410 System	a) Win NT 4.0 SP6a b) Win 2000 SP3 - Running NetDDE services	MS04-031	a) WindowsNT4Server-KB841533-x86-ENU.exe b) Windows2000-KB841533-x86-ENU.EXE	841533

Customers should subsequently contact their Kodak Service Representative for assistance in the installation of the software release. If required the Kodak Service organization will provide support for customers who choose to request assistance for these products. This will include the appropriate installation and operating verification for the products involved.

Customers that choose to download, install and verify operational performance for the products involved on their own, 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.

Complete Listing of Risks to Kodak Digital Capture 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
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	No known impact to Kodak products.
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	No known impact to Kodak products.
MS04-035	Critical	Remote Code Execution vulnerability exists in the Windows SMTP component	No known impact to Kodak products.

Vulnerability	Severity Rating	Impact of Vulnerability	Risk 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	No known impact 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	No known impact to Kodak products.