

# [NT] Vulnerability in Kodak Image Viewer Allows Code Execution (MS07-055)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-10/msg00011.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 10 Oct 2007 10:57:24 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>  
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.  
<http://www.securiteam.com/maillinglist.html>

-----

Vulnerability in Kodak Image Viewer Allows Code Execution (MS07-055)

---

## SUMMARY

A remote code execution vulnerability exists in the way that the Kodak Image Viewer, formerly known as Wang Image Viewer, handles specially crafted images files.

The vulnerability could allow an attacker to remotely execute code on the affected system. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

## DETAILS

Affected Software:

- \* Microsoft Windows 2000 Service Pack 4
- \* Windows XP Service Pack 2
- \* Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2

Operating System:

- \* Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition

## [NT] Vulnerability in Kodak Image Viewer Allows Code Execution (MS07-055)

### Service Pack 2

- \* Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems
- \* Windows Vista
- \* Windows Vista x64 Edition

### Kodak Image Viewer Remote Code Execution Vulnerability:

A remote code execution vulnerability exists in the way that the Kodak Image Viewer in Windows handles specially crafted image files. An attacker could exploit the vulnerability by constructing a specially crafted image that could potentially allow remote code execution if a user visited a Web site, viewed a specially crafted e-mail message, or opened an e-mail attachment. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

### Mitigating Factors for Kodak image Viewer Remote Code Execution Vulnerability:

Mitigation refers to a setting, common configuration, or general best-practice, existing in a default state, that could reduce the severity of exploitation of a vulnerability. The following mitigating factors may be helpful in your situation:

- \* Systems running Windows XP and Windows Server 2003 are only vulnerable if they were upgraded from Windows 2000.
- \* When Use Windows Classic Folders is enabled for viewing files, users are protected from shell-based attacks
- \* Office 2003 installs an image viewer application that takes over the file association, and is not vulnerable to this vulnerability.
- \* In a Web-based attack scenario, an attacker could host a Web site that contains a Web page that is used to exploit this vulnerability. In addition, compromised Web sites and Web sites that accept or host user-provided content or advertisements could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or Instant Messenger message that takes users to the attacker's Web site.
- \* An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

### Workarounds for Kodak image Viewer Remote Code Execution Vulnerability:

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces

functionality:

\* Read e-mail messages in plain text format to help protect yourself from the HTML e-mail attack vector

You can help protect yourself against this vulnerability by changing your e-mail settings to read e-mail messages in plain text using Outlook 2002 and later, Outlook Express 6 and later, or Windows Mail. For information in Outlook, search plain text in Help and review Read messages in plain text. In Outlook Express, search plain text in Help and review Reducing your risk of getting e-mail viruses. In Windows Mail, search plain text in Help and review Security and privacy in Windows Mail.

Impact of workaround: E-mail messages that are viewed in plain text format will not contain pictures, specialized fonts, animations, or other rich content. Additionally:

- \* The changes are applied to the preview pane and to open messages.
- \* Pictures become attachments so that they are not lost.
- \* Because the message is still in Rich Text or HTML format in the store, the object model (custom code solutions) may behave unexpectedly.
- \* Modify the access control list on oieng400.dll

To modify the Access Control List (ACL) on oieng400.dll to be more restrictive, follow these steps:

1. Log on as a user with administrator privileges.
2. Click Start, click Run, type cmd, and then click OK.
3. Document the current ACLs that are on the file (including inheritance settings) for future reference in case you have to undo this modification.

To view the ACLs, type the following:

```
cacls C:\winnt\system32\oieng400.dll
```

4. To deny the everyone group access to the file, type the following command at a command prompt:

```
cacls C:\winnt\system32\oieng400.dll /E /D Everyone
```

Impact of workaround: Kodak Image Viewer will not open.

How to undo the workaround: Restore the ACL that was documented in step 3 of this workaround.

FAQ for Kodak image Viewer Remote Code Execution Vulnerability:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system remotely. An attacker could then install programs or view, change, or delete data.

What causes the vulnerability?

## [NT] Vulnerability in Kodak Image Viewer Allows Code Execution (MS07-055)

The Windows Kodak image Viewer improperly parses specially crafted image files. As a result, memory may be corrupted in such a way that an attacker could execute arbitrary code in the context of the logged-on user.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could gain the same user rights as the local user. Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.

How could an attacker exploit the vulnerability?

An attacker could host a specially crafted Web site that is designed to exploit this vulnerability through Internet Explorer and then convince a user to view the Web site. This can also include compromised Web sites and Web sites that accept or host user-provided content or advertisements. These Web sites could contain specially crafted content that could exploit this vulnerability. In all cases, however, an attacker would have no way to force users to visit these Web sites. Instead, an attacker would have to convince users to visit the Web site, typically by getting them to click a link in an e-mail message or in an Instant Messenger request that takes users to the attacker's Web site. It could also be possible to display specially crafted Web content by using banner advertisements or by using other methods to deliver Web content to affected systems.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user view or open a specially crafted image file. Any system where applications use the affected Kodak image Viewer library to view or open image files are at risk.

What does the update do?

The update removes the vulnerability by improving the way that the Kodak image viewer handles specially crafted file types.

When this security bulletin was issued, had this vulnerability been publicly disclosed?

No. Microsoft received information about this vulnerability through responsible disclosure.

When this security bulletin was issued, had Microsoft received any reports that this vulnerability was being exploited?

No. Microsoft had not received any information to indicate that this vulnerability had been publicly used to attack customers and had not seen any examples of proof of concept code published when this security bulletin was originally issued.

CVE Information:

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2217>>  
CVE-2007-2217

### ADDITIONAL INFORMATION

[NT] Vulnerability in Kodak Image Viewer Allows Code Execution (MS07-055)

The information has been provided by Microsoft Security Bulletin MS07-055.

The original article can be found at:

<<http://www.microsoft.com/technet/security/bulletin/ms07-055.msp>>

<http://www.microsoft.com/technet/security/bulletin/ms07-055.msp>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@xxxxxxxxxxxxxx

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxx

=====

=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.