

[NT] Vulnerability in Windows Image Acquisition Service Allows Elevation of Privilege (MS07-007)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-02/msg00049.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxxxx>
 - *Date:* 15 Feb 2007 12:14:57 +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 Windows Image Acquisition Service Allows Elevation of Privilege (MS07-007)

SUMMARY

A privilege elevation vulnerability exists in Windows XP Service Pack 2 in the way that the Window Image Acquisition Service starts applications. This vulnerability could allow a logged on user to take complete control of the system.

DETAILS

Affected Software:

- * Microsoft Windows XP Service Pack 2 –

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=ce695e0e-938c-4fc6-a9a2-0eb9fc3e5512>>

Download the update

Non-Affected Software:

- * Microsoft Windows 2000 Service Pack 4
- * Microsoft Windows XP Professional x64 Edition
- * Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- * Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft

[NT] Vulnerability in Windows Image Acquisition Service Allows Elevation of Privilege (MS07-007)

Windows Server 2003 with SP1 for Itanium-based Systems

* Microsoft Windows Server 2003 x64 Edition

* Windows Vista

Mitigating Factors for Windows Image Acquisition Vulnerability – CVE-2007-0210:

* An attacker must have valid logon credentials and be able to log on locally to exploit this vulnerability. The vulnerability could not be exploited remotely or by anonymous users.

Workarounds for Windows Image Acquisition Vulnerability – CVE-2007-0210:

Microsoft has tested the following workarounds. Although these workarounds will not correct the underlying vulnerability, they help block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

* Disable the Windows Image Acquisition service

* Disabling the Windows Image Acquisition service will help protect the affected system from attempts to exploit this vulnerability. To disable the Windows Image Acquisition service, follow these steps:

1. Click Start, and then click Control Panel. Alternatively, point to Settings, and then click Control Panel.
2. Double-click Administrative Tools.
3. Double-click Services.
4. Double-click Windows Image Acquisition (WIA).
5. In the Startup type list, click Disabled.
6. Click Stop, and then click OK.

You can also stop and disable the Windows Image Acquisition (WIA) service by using the following command at the command prompt:

```
sc stop stisvc & sc config stisvc start= disabled
```

Impact of Workaround: If you disable the Windows Image Acquisition (WIA) service, you may not be able to connect or communicate with various imaging devices including digital cameras and scanners. Therefore, we recommend this workaround only on systems that do not require communication with digital imaging devices.

FAQ for Windows Image Acquisition Vulnerability – CVE-2007-0210:

What is the scope of the vulnerability?

This is a privilege elevation vulnerability. An attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. To attempt to exploit the vulnerability, an attacker must be able to log on locally to the system and run a program.

What causes the vulnerability?

An unchecked buffer in the Windows Image Acquisition service.

[NT] Vulnerability in Windows Image Acquisition Service Allows Elevation of Privilege (MS07-007)

What is Windows Image Acquisition Service (WIA)?

Windows Image Acquisition (WIA) enables imaging programs, such as Microsoft Picture It! 2000, Kodak Imaging, or Adobe Photoshop, to communicate with imaging devices such as digital cameras and scanners. WIA supports digital still cameras and both low-end and high-end scanners; it also enables you to retrieve still images from IEEE 1394-based digital video (DV) camcorders and Universal Serial Bus (USB) Web cameras.

What might an attacker use the vulnerability to do?

An attacker who successfully exploited this vulnerability could take complete control of the affected system.

How could an attacker exploit the vulnerability?

To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and gain complete control over the affected system.

What systems are primarily at risk from the vulnerability?

Windows XP Service Pack 2 systems are at risk from this vulnerability.

Could the vulnerability be exploited over the Internet?

No. An attacker must be able to log on locally to the specific system that is targeted for an attack.

What does the update do?

The update removes the vulnerability by modifying the way that the Windows Image Acquisition (WIA) validates the length of a message before it passes the message to the allocated buffer.

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.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security Bulletin MS07-007.

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms07-007.mspx>

<http://www.microsoft.com/technet/security/bulletin/ms07-007.mspx>

=====

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@xxxxxxxxxxxxxxxx

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

=====

=====

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.