

[NT] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution (MS06-001)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2006-01/msg00027.html>

- *From:* SecuriTeam <support@xxxxxxxxxxxxxx>
 - *Date:* 8 Jan 2006 14:06:16 +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 Graphics Rendering Engine Allows Remote Code Execution
(MS06-001)

SUMMARY

A remote code execution vulnerability exists in the Graphics Rendering Engine due to the way it handles Windows Metafile (WMF) images.

DETAILS

Vulnerable Systems:

* Microsoft Windows 2000 Service Pack 4

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=AA9E27BD-CB9A-4EF1-92A3-00FFE7B2AC74>>

Download the update

* Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=0C1B4C96-57AE-499E-B89B-215B7BB4D8E9>>

Download the update

* Microsoft Windows XP Professional x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=3A1166E6-5E9E-4E73-BCD4-28ECA6ECE877>>

Download the update

* Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1

[NT] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution (MS06-001)

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=1584AAE0-51CE-47D6-9A03-DB5B9077F1F2>>

Download the update

* Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=6E372D41-2C16-415E-8306-A5CA8845CC09>>

Download the update

* Microsoft Windows Server 2003 x64 Edition

<<http://www.microsoft.com/downloads/details.aspx?FamilyId=A8F4DCBA-5D28-4D9D-A6A4-3B71108CFE2D>>

Download the update

* Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) Review the FAQ section of this bulletin for details about these operating systems.

Graphics Rendering Engine Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560>>

CVE-2005-4560:

A remote code execution vulnerability exists in the Graphics Rendering Engine because of the way that it handles Windows Metafile (WMF) images. An attacker could exploit the vulnerability by constructing a specially crafted WMF image that could potentially allow remote code execution if a user visited a malicious Web site or opened a specially crafted attachment in e-mail. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Mitigating Factors for Graphics Rendering Engine Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560>>

CVE-2005-4560:

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. Also, Web sites that accept or host user-provided content or advertisements, and compromised Web sites, may contain malicious 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 persuade users to visit the Web site, typically by getting them to click a link in an e-mail or Instant Messenger request 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 Graphics Rendering Engine Vulnerability –

<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560>>

CVE-2005-4560:

Microsoft has tested the following workaround. While this workaround will not correct the underlying vulnerability, it will help block known attack vectors.

* Unregister the Windows Picture and Fax Viewer (Shimgvw.dll) on Windows XP Service Pack 1; Windows XP Service Pack 2; Windows Server 2003 and

Windows Server 2003 Service Pack 1

Microsoft has tested the following workaround. While this workaround will not correct the underlying vulnerability, it helps block known attack vectors. When a workaround reduces functionality, it is identified in the following section.

Note This workaround is intended to help protect against Web based exploit vectors and is not effective against exploits that have Windows Metafile images embedded in Word documents and other similar attack vectors.

Note The following steps require Administrative privileges. We recommend that you restart the computer after you apply this workaround. Alternatively, you can log out and log back in after you apply the workaround. However, we do recommend that you restart the computer.

To un-register Shimgvw.dll, follow these steps:

1. Click Start, click Run, type "regsvr32 -u %windir%\system32\shimgvw.dll" (without the quotation marks), and then click OK.
2. When a dialog box appears that confirms that the process has been successful, click OK.

Impact of Workaround: The Windows Picture and Fax Viewer will no longer start when users click a link to an image type that is associated with the Windows Picture and Fax Viewer.

To undo this workaround after the security update has been deployed, reregister Shimgvw.dll. To do this, use this same procedure, but replace the text in step 1 with "regsvr32 %windir%\system32\shimgvw.dll" (without the quotation marks).

FAQ for Graphics Rendering Engine Vulnerability –
<<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2005-4560>>
CVE-2005-4560:

What is the scope of the vulnerability?

This is a remote code execution vulnerability. If a user is logged on with administrative user rights, 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. 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.

What causes the vulnerability?

A vulnerability exists in the way that the Graphics Rendering Engine handles specially crafted WMF images that could allow arbitrary code to be executed.

[NT] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution (MS06-001)

What is the Windows Metafile (WMF) image format?

A Windows Metafile (WMF) image is a 16-bit metafile format that can contain both vector information and bitmap information. It is optimized for the Windows operating system.

For more information about image types and formats, see

<<http://support.microsoft.com/kb/320314>> Microsoft Knowledge Base Article 320314 or visit the

<<http://msdn.microsoft.com/library/default.asp?url=/library/en-us/gdicpp/GDIPlus/AboutGDIPlus/ImagesBitmapsandMSDNLibraryWebSite>> MSDN Library Web site.

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?

An attacker could exploit this vulnerability by creating a malicious Web page or a specially crafted attachment in e-mail and then persuading the user to visit the page or open the attachment. If the user visited the page or opened the attachment, the attacker could cause malicious code to run in the security context of the locally logged on user. 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.

An attacker could also attempt to exploit this vulnerability by embedding a specially crafted Windows Metafile (WMF) image within other files such as Word documents and convince a user to open this document.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and reading e-mail or visiting Web sites for any malicious action to occur. Therefore, any systems where e-mail is read or where Internet Explorer is used frequently, such as workstations or terminal servers, are at the most risk from this vulnerability. Systems that are not typically used to read e-mail or to visit Web sites, such as most server systems, are at a reduced risk.

Does this vulnerability affect image formats other than Windows Metafile (WMF)?

The only image format that is affected is the Windows Metafile (WMF) format. It is possible, however, that an attacker could rename the file name extension of a WMF file to that of a different image format. In this situation, it is likely that the Graphics Rendering Engine would detect and render the file as a WMF image, which could allow exploitation.

If I block files that use the .wmf file name extension, can this protect me against attempts to exploit this vulnerability?

No. The Graphics Rendering Engine does not determine file types by the file name extensions that they use. Therefore, if an attacker alters the file name extension of a WMF file, the Graphics Rendering Engine could

still render the file in a way that could exploit the vulnerability.

Does the workaround in this bulletin protect me from attempts to exploit this vulnerability through WMF images with changed extensions?

Yes. The workaround in this bulletin help protect against WMF images with changed extensions. This workaround is only effective in scenarios where the Windows Picture and Fax Viewer (Shimgvw.dll) would have been opened. This workaround is intended to help protect against Web based exploit vectors and is not effective against exploits that have Windows Metafile images embedded in Word documents and other similar attack vectors.

What systems are primarily at risk from the vulnerability?

Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who do not have sufficient administrative permissions are given the ability to log on to servers and to run programs. However, best practices strongly discourage allowing this.

Are Windows 98, Windows 98 Second Edition or Windows Millennium Edition critically affected by this vulnerability?

No. Although Windows Millennium Edition does contain the affected component, the vulnerability is not critical. For more information about severity ratings, visit the following <http://go.microsoft.com/fwlink/?LinkId=21140> Web site.

What does the update do?

The update removes the vulnerability by modifying the way that Windows Metafile (WMF) images are handled.

Specifically, the change introduced to address this vulnerability removes the support for the SETABORTPROC record type from the META_ESCAPE record in a WMF image. This update does not remove support for ABORTPROC functions registered by application SetAbortProc() API calls.

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

Yes. This vulnerability has been publicly disclosed. It has been assigned Common Vulnerability and Exposure number CVE-2005-4560.

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

Yes. When the security bulletin was released, Microsoft had received information that this vulnerability was being exploited.

Does applying this security update help protect customers from the code that has been published publicly that attempts to exploit this vulnerability?

Yes. This security update addresses the vulnerability that is currently being exploited. The vulnerability that has been addressed has been assigned the Common Vulnerability and Exposure number CVE-2005-4560.

What s Microsoft s response to the availability of third party patches for

[NT] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution (MS06-001)

the WMF vulnerability?

Microsoft recommends that customers download and deploy the security update associated with this security bulletin.

As a general rule, it is a best practice to obtain security updates for software vulnerabilities from the original vendor of the software. With Microsoft software, Microsoft carefully reviews and tests security updates to ensure that they are of high quality and have been evaluated thoroughly for application compatibility. In addition, Microsoft's security updates are offered in 23 languages for all affected versions of the software simultaneously.

Microsoft cannot provide similar assurance for independent third party security updates.

How does this vulnerability relate to the vulnerabilities that were corrected by MS05-053?

Both vulnerabilities were in the Graphics Rendering Engine. However, this update addresses a new vulnerability that was not addressed as part of MS05-053. MS05-053 helps protect against the vulnerability that is discussed in that bulletin, but does not address this new vulnerability. This update does not replace MS05-053. You must install this update and the update that is provided as part of the MS05-053 security bulletin to help protect your system against both vulnerabilities.

ADDITIONAL INFORMATION

The information has been provided by Microsoft Security.

The original article can be found at:

<<http://www.microsoft.com/technet/security/Bulletin/MS06-001.msp>>

<http://www.microsoft.com/technet/security/Bulletin/MS06-001.msp>

The original advisory can be found at:

<<http://www.microsoft.com/technet/security/advisory/912840.msp>>

<http://www.microsoft.com/technet/security/advisory/912840.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:

[NT] Vulnerability in Graphics Rendering Engine Allows Remote Code Execution (MS06-001)

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.

- Prev by Date: [\[UNIX\] Perl Module File::ExtAttr Buffer Overflow](#)
- Next by Date: [\[NT\] BlueCoat WinProxy Multiple DoS and Buffer Overflow](#)
- Previous by thread: [\[UNIX\] Perl Module File::ExtAttr Buffer Overflow](#)
- Next by thread: [\[NT\] BlueCoat WinProxy Multiple DoS and Buffer Overflow](#)
- Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)