

# [NT] Vulnerabilities in DirectX Allows Code Execution (MS07-064)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-12/msg00035.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 12 Dec 2007 13:03:42 +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>

-----

Vulnerabilities in DirectX Allows Code Execution (MS07-064)

---

## SUMMARY

This critical security update resolves two privately reported vulnerabilities in Microsoft DirectX. These vulnerabilities could allow code execution if a user opened a specially crafted file used for streaming media in DirectX.

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.

## DETAILS

Affected Software:

- \* DirectX 7.0 and DirectX 8.1
- \* Microsoft Windows 2000 Service Pack 4
  
- \* DirectX 9.0c

## [NT] Vulnerabilities in DirectX Allows Code Execution (MS07-064)

- \* Microsoft Windows 2000 Service Pack 4
- \* Windows XP Service Pack 2
- \* Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2
- \* Windows Server 2003 Service Pack1 and Windows Server 2003 Service Pack 2
- \* Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2
- \* Windows Server 2003 with SP1 & SP2 for Itanium-based Systems
  
- \* DirectX 10.0
- \* Windows Vista
- \* Windows Vista x64 Edition

### Microsoft DirectX Code Execution Vulnerability Parsing SAMI Files – CVE-2007-3901:

A remote code execution vulnerability exists in the way DirectX handles supported format files. This vulnerability could allow code execution if a user opened a specially crafted file. 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.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3901>>  
CVE-2007-3901.

### Mitigating Factors for Microsoft DirectX Code Execution Vulnerability Parsing SAMI Files – CVE-2007-3901:

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

- \* The vulnerability cannot be exploited automatically through e-mail when a user views or previews e-mail messages. For an attack to be successful, a user must open an attachment that is sent in an e-mail message.
  
- \* The vulnerability cannot be exploited through a Web-based attack scenario with Windows Media Player 6.4 on Windows 2000 Service Pack 4.

### Workarounds for Microsoft DirectX Code Execution Vulnerability Parsing SAMI Files – CVE-2007-3901:

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:

\* Modify the Access Control List for quartz.dll

On Windows XP (all editions), run the following command from a command prompt:

```
Echo y | Cacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /E /P everyone:N
```

On Windows Vista (all editions), run the following command from an elevated command prompt:

```
Takeown.exe /f %WINDIR%\SYSTEM32\QUARTZ.DLL  
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /save %TEMP%\QUARTZ_ACL.TXT  
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /deny everyone:(F)
```

Impact of workaround: WAV and AVI files will fail to play in DirectX-enabled applications on Windows Vista. All files will fail to play in DirectX-enabled applications on Windows XP.

How to undo the workaround: On Windows XP (all editions), run the following command from a command prompt:

```
Cacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /E /R everyone
```

On Windows Vista (all editions), run the following command from an elevated command prompt:

```
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /grant everyone:(F)  
Icacls.exe %WINDIR%\SYSTEM32 /restore %TEMP%\QUARTZ_ACL.TXT
```

\* Unregister the quartz.dll

```
Regsvr32.exe u %WINDIR%\SYSTEM32\QUARTZ.DLL
```

Impact of workaround: WAV and AVI files will fail to play in DirectX-enabled applications on Windows Vista. All files will fail to play in DirectX-enabled applications on Windows XP.

How to undo the workaround: Run the following command from an elevated command prompt:

```
Regsvr32.exe %WINDIR%\SYSTEM32\QUARTZ.DLL
```

FAQ for Microsoft DirectX Code Execution Vulnerability Parsing SAMI Files – CVE–2007–3901:

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; view, change, or delete data; or create new accounts with full user rights.

What causes the vulnerability?

Microsoft DirectShow, an intergraded technology of DirectX, does not

## [NT] Vulnerabilities in DirectX Allows Code Execution (MS07-064)

perform sufficient parsing of the parameters of Synchronized Accessible Media Interchange (SAMI) file types.

What is DirectShow?

Microsoft DirectShow is used for streaming media on Microsoft Windows operating systems. DirectShow is used for high-quality capture and playback of multimedia streams. It automatically detects and uses video and audio acceleration hardware when available, but also supports systems without acceleration hardware. DirectShow is also integrated with other DirectX technologies. Some examples of applications that you can create using DirectShow include DVD players, video editing applications, AVI to ASF converters, MP3 players, and digital video capture applications.

What is DirectX?

Microsoft DirectX is a feature of the Windows operating system. It is used for streaming media on Microsoft Windows operating systems to enable graphics and sound when playing games or watching video.

What might an attacker use the vulnerability to do?

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.

How could an attacker exploit the vulnerability?

Exploitation of this vulnerability would require a user to open a specially crafted format file. However, since the vulnerability is in the streaming component of Microsoft Windows, attacks can be launched from a specially crafted Web site or any application that delivers Web content.

What systems are primarily at risk from the vulnerability?

This vulnerability requires that a user is logged on and opens the specially crafted file. Workstations and terminal servers are primarily at risk. Servers could be at more risk if users who should 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.

What does the update do?

The update removes the vulnerability by increasing the validation that the DirectX parser performs on supported 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

## [NT] Vulnerabilities in DirectX Allows Code Execution (MS07-064)

any examples of proof of concept code published when this security bulletin was originally issued.

### Microsoft DirectX Code Execution Vulnerability Parsing WAV and AVI Files CVE-2007-3895:

A remote code execution vulnerability exists in the way DirectX handles WAV and AVI format files. This vulnerability could allow code execution if a user visits a specially crafted Web site or opens an e-mail message with specially crafted content. 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.

To view this vulnerability as a standard entry in the Common Vulnerabilities and Exposures list, see

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3895>.>  
CVE-2007-3895.

### Mitigating Factors for Microsoft DirectX Code Execution Vulnerability Parsing WAV and AVI Files – CVE-2007-3895:

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:

\* 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.

\* In an e-mail-based attack of this exploit, customers who read e-mail in plain text are at less risk from this vulnerability.

### Workarounds for Microsoft DirectX Code Execution Vulnerability Parsing WAV and AVI Files – CVE-2007-3895:

Workaround refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack

## [NT] Vulnerabilities in DirectX Allows Code Execution (MS07-064)

vectors before you apply the update. Microsoft has tested the following workarounds and states in the discussion whether a workaround reduces functionality:

\* Modify the Access Control List for quartz.dll

On Windows XP (all editions), run the following command from a command prompt:

```
Echo y| Cacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /E /P everyone:N
```

On Windows Vista (all editions), run the following command from an elevated command prompt:

```
Takeown.exe /f %WINDIR%\SYSTEM32\QUARTZ.DLL  
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /save %TEMP%\QUARTZ_ACL.TXT  
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /deny everyone:(F)
```

Impact of workaround: WAV and AVI files will fail to play in DirectX-enabled applications on Windows Vista. All files will fail to play in DirectX-enabled applications on Windows XP.

How to undo the workaround: On Windows XP (all editions), run the following command from a command prompt:

```
Cacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /E /R everyone
```

On Windows Vista (all editions), run the following command from an elevated command prompt:

```
Icacls.exe %WINDIR%\SYSTEM32\QUARTZ.DLL /grant everyone:(F)  
Icacls.exe %WINDIR%\SYSTEM32\restore %TEMP%\QUARTZ_ACL.TXT
```

\* Unregister the quartz.dll

```
Regsvr32.exe u %WINDIR%\SYSTEM32\QUARTZ.DLL
```

Impact of workaround: WAV and AVI files will fail to play in DirectX-enabled applications on Windows Vista. All files will fail to play in DirectX-enabled applications on Windows XP.

How to undo the workaround: Run the following command from an elevated command prompt:

```
Regsvr32.exe %WINDIR%\SYSTEM32\QUARTZ.DLL
```

FAQ for Microsoft DirectX Code Execution Vulnerability Parsing WAV and AVI Files – CVE-2007-3895:

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; view, change, or delete data; or create new accounts with full user rights.

## [NT] Vulnerabilities in DirectX Allows Code Execution (MS07-064)

What causes the vulnerability?

DirectShow, an intergraded technology of DirectX, does not perform sufficient validation of WAV and AVI file parameters.

What is DirectShow?

Microsoft DirectShow is used for streaming media on Microsoft Windows operating systems. DirectShow is used for high-quality capture and playback of multimedia streams. It automatically detects and uses video and audio acceleration hardware when available, but also supports systems without acceleration hardware. It is also integrated with other DirectX technologies. Some of the types of applications that you can create by using DirectShow include DVD players, video editing applications, AVI to ASF converters, MP3 players, and digital video capture applications.

What is DirectX?

Microsoft DirectX is a feature of the Windows operating system. It is used for streaming media on Microsoft Windows operating systems to enable graphics and sound when playing games or watching video.

What might an attacker use the vulnerability to do?

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.

How could an attacker exploit the vulnerability?

Exploitation of this vulnerability would require a user to open a specially crafted format file. However, since the vulnerability is in the streaming component of Microsoft Windows, attacks can be launched from a specially crafted Web site or applications that deliver Web content.

What systems are primarily at risk from the vulnerability?

Exploitation of this vulnerability would require a user to open a specially crafted format file. However, since the vulnerability can be triggered by Windows Media Player or other media player with Web-based playback functionality, attacks can be launched from a specially crafted Web site or applications that deliver Web content.

What does the update do?

The update removes the vulnerability by increasing the validation that the DirectShow parser performs on supported 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

[NT] Vulnerabilities in DirectX Allows Code Execution (MS07-064)

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 MS07-064.

The original article can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms07-064.mspx>

<http://www.microsoft.com/technet/security/bulletin/ms07-064.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@xxxxxxxxxxxxxxx

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

=====

=====

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.