



CVE-2007-3901

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2007-3901
State	PUBLISHED
Assigner	microsoft
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-12-12 00:46:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Stack-based buffer overflow in the DirectShow Synchronized Accessible Media Interchange (SAMI) parser in quartz.dll for M

Risk And Classification

Primary CVSS: v2.0 8.5 from nvd@nist.gov

AV:N/AC:M/Au:S/C:C/I:C/A:C

Problem Types: CWE-119 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

Complete

Integrity

Complete

Availability

Complete

AV:N/AC:M/Au:S/C:C/I:C/A:C

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Directx	10.0	All	All	All

Application	Microsoft	Directx	5.2	All	All	All
Application	Microsoft	Directx	6.1	All	All	All
Application	Microsoft	Directx	7.0	All	All	All
Application	Microsoft	Directx	7.0a	All	All	All
Application	Microsoft	Directx	7.1	All	All	All
Application	Microsoft	Directx	8.0	All	All	All
Application	Microsoft	Directx	8.0a	All	All	All
Application	Microsoft	Directx	8.1	All	All	All
Application	Microsoft	Directx	8.1a	All	All	All
Application	Microsoft	Directx	8.1b	All	All	All
Application	Microsoft	Directx	8.2	All	All	All
Application	Microsoft	Directx	9.0a	All	All	All
Application	Microsoft	Directx	9.0b	All	All	All
Application	Microsoft	Directx	9.0c	All	All	All
Operating System	Microsoft	Windows 2000	All	All	All	All
Operating System	Microsoft	Windows 2003 Server	datacenter_edition	All	All	All
Operating System	Microsoft	Windows 2003 Server	enterprise_edition	All	All	All
Operating System	Microsoft	Windows 2003 Server	standard	All	All	All
Operating System	Microsoft	Windows 2003 Server	web_edition	All	All	All
Operating System	Microsoft	Windows Vista	All	All	All	All
Operating System	Microsoft	Windows Xp	All	All	home	All
Operating System	Microsoft	Windows Xp	All	All	professional	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Microsoft Security Bulletin MS07-064 - Critical Microsoft Docs	af8
Microsoft DirectX SAMI File Parsing - Remote Stack Overflow - Windows remote Exploit	af8
Microsoft DirectX SAMI File Parsing Stack Buffer Overflow Vulnerability	af8
Microsoft DirectX SAMI/WAV/AVI File Parsing Vulnerabilities - Advisories - Secunia	af8
Webmail - OVH	af8
IBM X-Force Exchange	af8
Multiple Microsoft DirectShow Vulnerabilities	af8
SecurityTracker.com Archive: Microsoft DirectX Bugs in Parsing SAMI, WAV, and AVI Files Let Remote Users Execute Arbitrary Code	af8

SecurityTracker.com Archives - Microsoft DirectX Bugs in Parsing SAMI, WAV, and AVI Files Let Remote Users Execute Arbitrary Code	atc
labs.iddefense.com/intelligence/vulnerabilities/display.php	af8
US-CERT Technical Cyber Security Alert TA07-345A -- Microsoft Updates for Multiple Vulnerabilities	af8
SecurityFocus	af8
Repository / Oval Repository	af8
US-CERT Vulnerability Note VU#804089	af8
CVE Program record	CV
NVD vulnerability detail	NV

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)