CVE-2008-0015

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2008-0015
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-07-07 23:30:00 UTC
Updated	2026-04-21 18:41:48 UTC
Description	Stack-based buffer overflow in the CComVariant::ReadFromStream function in the Active Template Library (ATL), as used

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

EPSS: 0.831720000 probability, percentile 0.992660000 (date 2026-04-21)

CISA KEV: Listed on 2026-02-17; due 2026-03-10; ransomware use Unknown

Problem Types: CWE-119 | CWE-121 | n/a | CWE-121 CWE-121 Stack-based Buffer Overflow

Version	Source	Type	Score	Severity	Vector
3.1	ADP	DECLARED	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	9.3		AV:N/AC:M/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Microsoft
Product	Windows
Name	Microsoft Windows Video ActiveX Control Remote Code Execution Vulnerability
Required Action	Apply mitigations per vendor instructions, follow applicable BOD 22-01 guidance for cloud services, or discontinue use of the product if mitigations are unavailable.
Notes	https://web.archive.org/web/20110305211119/https://www.microsoft.com/technet/security/bulletin/ms09-032.mspx ; https://nvd.nist.gov/vuln/detail/CVE-2008-0015

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows 2003 Server	-	sp2	All	All
Operating System	Microsoft	Windows 2003 Server	-	sp2	itanium	All
Operating System	Microsoft	Windows 2003 Server	-	sp2	x64	All
Operating System	Microsoft	Windows Xp	-	sp2	All	All
Operating System	Microsoft	Windows Xp	-	sp3	All	All

Vendor Declared Affected Products

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

References

Reference	Sourc
Microsoft Security Bulletin MS09-032 - Critical | Microsoft Docs	af854a
Repository / Oval Repository	af854a
US-CERT Technical Cyber Security Alert TA09-187A -- Microsoft Video ActiveX Control Vulnerability	af854a
Your request has been blocked. This could be due to several reasons.	af854a
Microsoft Video Control ActiveX Remote Code Execution	af854a
Microsoft Active Template Library Header Data Remote Code Execution Vulnerability	af854a
VU#180513 - Microsoft Video ActiveX control stack buffer overflow	af854a
Repository / Oval Repository	af854a
Microsoft Active Template Library 'IPersistStreamInit' Remote Code Execution Vulnerability	af854a
Microsoft Windows Various Components ATL Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com	af854a
SecurityTracker.com Archives - Microsoft DirectShow Buffer Overflow in ActiveX Control Lets Remote Users Execute Arbitrary Code	af854a
www.csis.dk/dk/nyheder/nyheder.asp	af854a
osvdb.org/55651	af854a
US-CERT Technical Cyber Security Alert TA09-223A -- Microsoft Updates for Multiple Vulnerabilities	af854a
Repository / Oval Repository	af854a
MS09-037: Why we are using CVE's already used in MS09-035 - Security Research & Defense - Site Home - TechNet Blogs	af854a
Microsoft Security Bulletin MS09-037 - Critical | Microsoft Docs	af854a
US-CERT Technical Cyber Security Alert TA09-195A -- Microsoft Updates for Multiple Vulnerabilities	af854a
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a
0-day in Microsoft DirectShow (msvidctl.dll) used in drive-by attacks	af854a
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c7(
CVE Program record	CVE.C
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event

ADP	2026-02-17T00:00:00.000Z	CVE-2008-0015 added to CISA KEV

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**