CVE-2009-4324

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

Summary

CVE	CVE-2009-4324
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-12-15 02:30:00 UTC
Updated	2026-04-21 21:12:37 UTC
Description	Use-after-free vulnerability in the Doc.media.newPlayer method in Multimedia.api in Adobe Reader and Acrobat 9.x before

Risk And Classification

Primary CVSS: v3.1 7.8 HIGH from nvd@nist.gov

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

EPSS: 0.928640000 probability, percentile 0.997720000 (date 2026-05-09)

CISA KEV: Listed on 2022-06-08; due 2022-06-22; ransomware use Unknown

Problem Types: CWE-416 | n/a | CWE-416 CWE-416 Use After Free

Version	Source	Type	Score	Severity	Vector
3.1	nvd@nist.gov	Primary	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	ADP	DECLARED	7.8	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
3.1	134c704f-9b21-4f2e-91b3-4a467353bcc0	Secondary	7.8	HIGH	CVSS:3.1/AV:L/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

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.1/AV:L/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	Adobe
Product	Acrobat and Reader
Name	Adobe Acrobat and Reader Use-After-Free Vulnerability
Required Action	Apply updates per vendor instructions.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2009-4324

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Acrobat	All	All	All	All

Vendor Declared Affected Products

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

References

Reference
IBM X-Force Exchange
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Red Hat update for acroread - Advisories - Community
www.cisa.gov/known-exploited-vulnerabilities-catalog
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
Adobe Reader/Acrobat Memory Corruption Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
Zero-Day Xmas Present | Symantec Connect
Metasploit Framework - /modules/exploits/windows/fileformat/adobe_media_newplayer.rb - Metasploit Redmine Interface
US-CERT Vulnerability Note VU#508357
Adobe - Security Bulletin APSB10-02 Security updates available for Adobe Reader and Acrobat
547799 – (CVE-2009-4324) CVE-2009-4324 acroread: media.newplayer JavaScript API code execution vulnerability (APSB10-02)
Support
Adobe Reader and Acrobat 'newplayer()' JavaScript Method Remote Code Execution Vulnerability
contagio: Dec.11 Adobe 0 day CVE-2009-4324 Attack of the Day (#1). Fwd: Reference from christanderson.ma@gmail.com Fri 2009-12-11 0
Adobe Reader/Acrobat 7 Multiple Vulnerabilities - Secunia Advisories - Vulnerability Information - Secunia.com
Adobe - Security Advisories: APSA09-07 - Security Advisory for Adobe Reader and Acrobat
[security-announce] SUSE Security Announcement: acoread (SUSE-SA:2010:00
osvdb.org/60980
New Adobe Reader and Acrobat Vulnerability - Adobe Product Security Incident Response Team (PSIRT)
Shadowserver Foundation - Calendar - 2009-12-14
Repository / Oval Repository
US-CERT Technical Cyber Security Alert TA10-013A -- Adobe Reader and Acrobat Vulnerabilities
CVE Program record
NVD vulnerability detail
CISA Known Exploited Vulnerabilities catalog

No vendor comments have been submitted for this CVE.

Additional Advisory Data

Source	Time	Event
ADP	2022-06-08T00:00:00.000Z	CVE-2009-4324 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