CVE-2011-0609

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

Summary

CVE	CVE-2011-0609
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-03-15 17:55:03 UTC
Updated	2026-04-21 20:30:17 UTC
Description	Unspecified vulnerability in Adobe Flash Player 10.2.154.13 and earlier on Windows, Mac OS X, Linux, and Solaris; 10.1.1(

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: 0.920790000 probability, percentile 0.997170000 (date 2026-05-17)

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

Problem Types: NVD-CWE-noinfo | n/a | CWE-noinfo Not enough information

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	Flash Player
Name	Adobe Flash Player Unspecified Vulnerability
Required Action	The impacted product is end-of-life and should be disconnected if still in use.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2011-0609

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Acrobat	10.0	All	All	All
Application	Adobe	Acrobat	10.0.1	All	All	All
Application	Adobe	Acrobat	All	All	All	All
Application	Adobe	Acrobat Reader	10.0	All	All	All
Application	Adobe	Acrobat Reader	10.0.1	All	All	All
Application	Adobe	Acrobat Reader	All	All	All	All

Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Google	Android	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Oracle	Solaris	-	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
SecurityTracker: Adobe Reader and Acrobat Flaw in 'authplay.dll' Lets Remote Users Execute Arbitrary Code	af854a3a-2127-422b-91ae
Adobe Flash Player / AIR AVM2 Instruction Sequence Handling Vulnerability - Secunia.com	af854a3a-2127-422b-91ae
Background on APSA11-01 Patch Schedule « Adobe Secure Software Engineering Team (ASSET) Blog	af854a3a-2127-422b-91ae
Adobe - Security Bulletins: APSB11-06 - Security updates available for Adobe Reader and Acrobat	af854a3a-2127-422b-91ae
Adobe - Security Advisories: APSA11-01 - Security Advisory for Adobe Flash Player, Adobe Reader and Acrobat	af854a3a-2127-422b-91ae
Adobe Reader/Acrobat authplay.dll AVM2 Instruction Sequence Handling Vulnerability - Secunia.com	af854a3a-2127-422b-91ae
access.redhat.com	af854a3a-2127-422b-91ae
SecurityTracker: Adobe AIR Flaw Lets Remote Users Execute Arbitrary Code	af854a3a-2127-422b-91ae
SecurityTracker: Adobe Flash Player Flaw Lets Remote Users Execute Arbitrary Code	af854a3a-2127-422b-91ae
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3
IBM X-Force Exchange	af854a3a-2127-422b-91ae
Adobe Flash Player AVM Bytecode Verification - SecurityReason.com	af854a3a-2127-422b-91ae
[security-announce] SUSE Security Summary Report: SUSE-SR:2011:005	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
Chrome Releases: Stable and Beta Channel Updates	af854a3a-2127-422b-91ae
Repository / Oval Repository	af854a3a-2127-422b-91ae
US-CERT Vulnerability Note VU#192052 - Adobe Flash Player contains unspecified code execution vulnerability	af854a3a-2127-422b-91ae
Red Hat update for flash-plugin - Secunia.com	af854a3a-2127-422b-91ae
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae
Adobe Flash Player CVE-2011-0609 'SWF' File Remote Memory Corruption Vulnerability	af854a3a-2127-422b-91ae

Google Chrome Flash Player AVM2 Instruction Sequence Handling Vulnerability - Secunia.com	af854a3a-2127-422b-91ae
CVE Program record	CVE.ORG
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	2022-06-08T00:00:00.000Z	CVE-2011-0609 added to CISA KEV

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 registred 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**