CVE-2016-4117

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

Summary

CVE	CVE-2016-4117
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-05-11 01:59:46 UTC
Updated	2026-04-21 21:07:21 UTC
Description	Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors, as exp

Risk And Classification

Primary CVSS: v3.1 9.8 CRITICAL from nvd@nist.gov

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

EPSS: 0.930520000 probability, percentile 0.997900000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; 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	9.8	CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/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	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

CISA Known Exploited Vulnerability

Vendor	Adobe
Product	Flash Player
Name	Adobe Flash Player Arbitrary Code Execution 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-2016-4117

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	All	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All

Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server From Rhui	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Desktop	12	sp1	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	-	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	sp1	All	All

Vendor Declared Affected Products

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

References

Reference	Source
github.com/cisagov/vulnrichment/issues/196	134c704f-9b21-4f2e-91b3-4a4673
Adobe Flash Player: Multiple vulnerabilities (GLSA 201606-08) — Gentoo security	af854a3a-2127-422b-91ae-364da2
Adobe Security Bulletin	af854a3a-2127-422b-91ae-364da2
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2
Adobe Flash Player CVE-2016-4117 Unspecified Remote Code Execution Vulnerability	af854a3a-2127-422b-91ae-364da2
Adobe Flash Player Type Confusion Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da2
[security-announce] openSUSE-SU-2016:1308-1: important: Security update	af854a3a-2127-422b-91ae-364da2
[security-announce] SUSE-SU-2016:1305-1: important: Security update for	af854a3a-2127-422b-91ae-364da2
[security-announce] openSUSE-SU-2016:1306-1: important: Security update	af854a3a-2127-422b-91ae-364da2
[security-announce] openSUSE-SU-2016:1309-1: important: Security update	af854a3a-2127-422b-91ae-364da2
Adobe Security Advisory	af854a3a-2127-422b-91ae-364da2
Adobe Flash Player - DeleteRangeTimelineOperation Type Confusion (Metasploit) - OSX remote Exploit	af854a3a-2127-422b-91ae-364da2
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a4673
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
CISA Known Exploited Vulnerabilities catalog	CISA

No vendor comments have been submitted for this CVE.

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