CVE-2016-0984

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

Summary

CVE	CVE-2016-0984
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-02-10 20:59:32 UTC
Updated	2026-04-22 13:01:44 UTC
Description	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and

Risk And Classification

Primary CVSS: v3.1 8.8 HIGH from nvd@nist.gov

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

EPSS: 0.673450000 probability, percentile 0.985820000 (date 2026-05-17)

CISA KEV: Listed on 2022-05-25; due 2022-06-15; 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	8.8	HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
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	Adobe
Product	Flash Player and AIR
Name	Adobe Flash Player and AIR Use-After-Free Vulnerability
Required Action	The impacted products are end-of-life and should be disconnected if still in use.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2016-0984

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Operating System	Microsoft	Windows	-	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms

CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a467353bcc0
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2661108
[security-announce] openSUSE-SU-2016:0415-1: important: Security update	af854a3a-2127-422b-91ae-364da2661108
[security-announce] SUSE-SU-2016:0398-1: important: Security update for	af854a3a-2127-422b-91ae-364da2661108
Adobe Flash Player: Multiple vulnerabilities (GLSA 201603-07) — Gentoo Security	af854a3a-2127-422b-91ae-364da2661108
[security-announce] SUSE-SU-2016:0400-1: important: Security update for	af854a3a-2127-422b-91ae-364da2661108
Adobe Flash - Sound.loadPCMFromByteArray Dangling Pointer - Multiple dos Exploit	af854a3a-2127-422b-91ae-364da2661108
Adobe Flash Player Multiple Bugs Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da2661108
Adobe Security Bulletin	af854a3a-2127-422b-91ae-364da2661108
[security-announce] openSUSE-SU-2016:0412-1: important: Security update	af854a3a-2127-422b-91ae-364da2661108
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	2022-05-25T00:00:00.000Z	CVE-2016-0984 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**