CVE-2015-0313

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

Summary

CVE	CVE-2015-0313
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-02 19:59:00 UTC
Updated	2026-04-21 21:09:17 UTC
Description	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows a

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: 0.925440000 probability, percentile 0.997450000 (date 2026-05-02)

CISA KEV: Listed on 2022-04-13; due 2022-05-04; 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	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 Use-After-Free 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-2015-0313

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	All	All	All	All
Operating System	Linux	Linux Kernel	-	All	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-
Adobe Flash Player ByteArray With Workers Use After Free ≈ Packet Storm	af854a3a-2127-422b-91ae
www.osvdb.org/117853	af854a3a-2127-422b-91ae
Adobe Flash Player CVE-2015-0313 Remote Code Execution Vulnerability	af854a3a-2127-422b-91ae
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-
[security-announce] SUSE-SU-2015:0239-1: critical: Security update for f	af854a3a-2127-422b-91ae
Adobe Flash Player Use-After-Free Memory Error Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae
[security-announce] SUSE-SU-2015:0236-1: critical: Security update for f	af854a3a-2127-422b-91ae
Adobe Security Bulletin	af854a3a-2127-422b-91ae
[security-announce] openSUSE-SU-2015:0237-1: critical: Security update f	af854a3a-2127-422b-91ae
Adobe Security Bulletin	af854a3a-2127-422b-91ae
[security-announce] openSUSE-SU-2015:0238-1: critical: update for flash-	af854a3a-2127-422b-91ae
IBM X-Force Exchange	af854a3a-2127-422b-91ae
Microsoft Security Advisory 2755801	af854a3a-2127-422b-91ae
Security Advisory SA62777 - Microsoft Windows Flash Player Multiple Vulnerabilities - Secunia	af854a3a-2127-422b-91ae
About Secunia Research | Flexera	af854a3a-2127-422b-91ae
Adobe Flash Player ByteArray With Workers Use After Free	af854a3a-2127-422b-91ae
Security Advisory SA62895 - SUSE update for flash-player - Secunia	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.

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

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