CVE-2015-5119

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

Summary

CVE	CVE-2015-5119
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-08 14:59:05 UTC
Updated	2026-04-21 21:08:50 UTC
Description	Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x thr

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: 0.931500000 probability, percentile 0.997990000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; 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-2015-5119

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
Application	Adobe	Flash Player	All	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	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 Eus	6.6	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 Aus	6.6	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	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	-	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	-	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-91b3-4
Vulnerability Note VU#561288 - Adobe Flash ActionScript 3 ByteArray use-after-free vulnerability	af854a3a-2127-422b-91ae-
Adobe Flash Player ActionScript 3 ByteArray Use After Free Remote Memory Corruption Vulnerability	af854a3a-2127-422b-91ae-
[security-announce] openSUSE-SU-2015:1210-1: critical: Security update f	af854a3a-2127-422b-91ae-
Gentoo Security	af854a3a-2127-422b-91ae-
CVE-2015-5119 Adobe Flash Player ByteArray Use After Free | Rapid7	af854a3a-2127-422b-91ae-
Adobe Flash Player Use-After-Free Memory Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-
Hacking Team Leak Includes Multiple Exploits	af854a3a-2127-422b-91ae-
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4
Adobe Flash and Microsoft Windows Vulnerabilities | US-CERT	af854a3a-2127-422b-91ae-
Red Hat Customer Portal	af854a3a-2127-422b-91ae-
Adobe Security Bulletin	af854a3a-2127-422b-91ae-

JavaScript is not available.	af854a3a-2127-422b-91ae-
[security-announce] SUSE-SU-2015:1211-1: critical: Security update for f	af854a3a-2127-422b-91ae-
[security-announce] openSUSE-SU-2015:1207-1: critical: Security update f	af854a3a-2127-422b-91ae-
[security-announce] SUSE-SU-2015:1214-1: critical: Security update for f	af854a3a-2127-422b-91ae-
Adobe Flash Player ByteArray Use After Free ≈ Packet Storm	af854a3a-2127-422b-91ae-
Adobe Security Bulletin	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.

Free CVE JSON API cve.report/api

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