CVE-2015-7645

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

Summary

CVE	CVE-2015-7645
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-15 10:59:10 UTC
Updated	2026-04-22 12:22:49 UTC
Description	Adobe Flash Player 18.x through 18.0.0.252 and 19.x through 19.0.0.207 on Windows and OS X and 11.x through 11.2.202

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: 0.845260000 probability, percentile 0.993340000 (date 2026-04-22)

CISA KEV: Listed on 2022-03-03; due 2022-03-24; ransomware use Known

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 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-2015-7645

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	19.0.0.185	All	All	All
Application	Adobe	Flash Player	19.0.0.207	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	6.7	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	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
Adobe Flash - 'IExternalizable.writeExternal' Type Confusion - Multiple dos Exploit	af854a3a-2127-422b-91ae-364da2
Adobe Flash Player Type Confusion Errors Let Remote Users Execute Arbitrary Code - SecurityTracker	af854a3a-2127-422b-91ae-364da2
Adobe Security Bulletin	af854a3a-2127-422b-91ae-364da2
[security-announce] SUSE-SU-2015:1771-1: critical: Security update for f	af854a3a-2127-422b-91ae-364da2
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2
Adobe Flash IExternalizable.writeExternal Type Confusion ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2
Adobe Security Bulletin	af854a3a-2127-422b-91ae-364da2
[security-announce] openSUSE-SU-2015:1781-1: critical: Security update f	af854a3a-2127-422b-91ae-364da2
[security-announce] openSUSE-SU-2015:1768-1: critical: Security update f	af854a3a-2127-422b-91ae-364da2
Adobe Flash Player CVE-2015-7645 Remote Code Execution Vulnerability	af854a3a-2127-422b-91ae-364da2
New Adobe Flash Zero-Day Used in Pawn Storm Campaign Targeting Foreign Affairs Ministries	af854a3a-2127-422b-91ae-364da2
www.cisa.gov/known-exploited-vulnerabilities-catalog	134c704f-9b21-4f2e-91b3-4a46735

[security-announce] SUSE-SU-2015:1770-1: critical: Security update for f	af854a3a-2127-422b-91ae-364da2
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2
Adobe Flash Player: Multiple vulnerabilities (GLSA 201511-02) — Gentoo Security	af854a3a-2127-422b-91ae-364da2
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	2022-03-03T00:00:00.000Z	CVE-2015-7645 added to CISA KEV

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