CVE-2015-7653

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

Summary

CVE	CVE-2015-7653
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-11-11 12:59:52 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Air	All	All	All	All

Application	Adobe	Air	All	All	All	All
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	19.0.0.226	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	Google	Android	All	All	All	All
Operating System	Linux	Linux Kernel	-	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	Sourc
Red Hat Customer Portal	af854
Red Hat Customer Portal	af854
Adobe Security Bulletin	af854
openSUSE-SU-2015:1984-1: moderate: Security update for flash-player	af854
Adobe Flash Player and AIR APSB15-28 Multiple Use After Free Remote Code Execution Vulnerabilities	af854
ZDI-15-561 | Zero Day Initiative	af854
Adobe Flash Player: Multiple vulnerabilities (GLSA 201511-02) — Gentoo Security	af854
Adobe Flash Player Multiple Bugs Let Remote Users Write Data and Execute Arbitrary Code on the Target System - SecurityTracker	af854
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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**