CVE-2015-7630

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

Summary

CVE	CVE-2015-7630
State	PUBLISHED
Assigner	adobe
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-10-15 00:00:05 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux

Risk And Classification

Primary CVSS: v2.0 10 from nvd@nist.gov

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

Problem Types: CWE-119 | n/a

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Air	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	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
[security-announce] openSUSE-SU-2015:1744-1: important: Security update
Adobe Flash Player Multiple Bugs Let Remote Users Bypass Same-Origin Restrictions, Obtain Potentially Sensitive Information, and Execute
[security-announce] SUSE-SU-2015:1740-1: important: Security update for
Red Hat Customer Portal
[security-announce] openSUSE-SU-2015:1781-1: critical: Security update f
Adobe Security Bulletin
Adobe Flash Player and AIR APSB15-25 Multiple Unspecified Memory Corruption Vulnerabilities
Red Hat Customer Portal
Adobe Flash Player: Multiple vulnerabilities (GLSA 201511-02) — Gentoo Security
[security-announce] SUSE-SU-2015:1742-1: important: Security update for
CVE Program record
NVD vulnerability detail

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