

CVE-2014-0502

Adobe Flash Player Double Free Vulnerability

CISA KEV since Sep 17, 2024

Actively exploited

Double free vulnerability in Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in February 2014.

EVRS 75_{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.248 97.9th percentile · FIRST	CISA DEADLINE Oct 8, 2024 KEV since 2024 · listed over a year
---	--	--	---

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.248 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle Patch or fixed version identified

CISA required action: The impacted product is end-of-life (EoL) and/or end-of-service (EoS). Users should discontinue utilization of the product.

Basis: CISA KEV required action

Affected and fixed versions · 6 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	< 11.7.700.269 ≥ 11.8.800.94 < 12.0.0.70 < 11.2.202.341	11.7.700.269 · 12.0.0.70 · 11.2.202.341	NVD
adobe air sdk	< 4.0.0.1628	4.0.0.1628	NVD
adobe air	< 4.0.0.1628	4.0.0.1628	NVD
mac os x	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
android	—	no fixed version listed	NVD
opensuse	11.4 12.3 13.1	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-955p-xvq6-xggj

NVD nvd.nist.gov/vuln/detail/CVE-2014-0502

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2014-0533

adobe.com adobe.com/products/flashplayer/end-of-life-alternative.html#eol-alternative-faq

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

Current data evulnable.com/vulnerability-management/cve/CVE-2014-0502

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.