

CVE-2012-2034

Adobe Flash Player Memory Corruption Vulnerability

CISA KEV since Mar 28, 2022

Actively exploited

Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-2037.

EVRS 75/₁₀₀ Urgent priority	CVSS V3.1 7.5 High · NVD	EPSS 0.077 94.6th percentile · FIRST	CISA DEADLINE Apr 18, 2022 KEV since 2022 · 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	0.077 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.5	☐ 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 and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions · 5 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	≤ 11.2.202.235 ≤ 11.1.115.8 ≤ 11.1.111.9	after 11.2.202.235 · after 11.1.115.8 · after 11.1.111.9	NVD
air	≤ 3.2.0.2070	after 3.2.0.2070	NVD
macos	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
android	≥ 4.0 ≤ 4.4.4 ≥ 2.0 ≤ 3.2.6	no fixed version listed	NVD
opensuse	11.4 12.1	no fixed version listed	NVD
linux enterprise desktop	10 11	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-3cfr-rpp6-j86f	NVD	nvd.nist.gov/vuln/detail/CVE-2012-2034
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2012-2040
Current data	evulnable.com/vulnerability-management/cve/CVE-2012-2034		

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