

CVE-2016-0984

Adobe Flash Player and AIR Use-After-Free Vulnerability

CISA KEV since May 25, 2022

Actively exploited

Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0983.

EVRS 75_{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.545 99.02nd percentile · FIRST	CISA DEADLINE Jun 15, 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	0.545 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 products are end-of-life and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions · 3 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	≤ 20.0.0.272 ≤ 11.2.202.559 ≤ 18.0.0.326 ≤ 20.0.0.286	after 20.0.0.272 · after 11.2.202.559 · after 18.0.0.326 · after 20.0.0.286	NVD
flash player desktop runtime	≤ 20.0.0.286	after 20.0.0.286	NVD
air desktop runtime	≤ 20.0.0.233	after 20.0.0.233	NVD
air sdk	≤ 20.0.0.233	no fixed version listed	NVD
air sdk \& compiler	≤ 20.0.0.233	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
mac os x	—	no fixed version listed	NVD

Sources

Vendor guidance	helpx.adobe.com/security/products/flash-player/apsb16-04.html	NVD	nvd.nist.gov/vuln/detail/CVE-2016-0984
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-0994
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-0984		

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