

CVE-2016-7855

Adobe Flash Player Use-After-Free Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Use-after-free vulnerability in Adobe Flash Player before 23.0.0.205 on Windows and OS X and before 11.2.202.643 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in October 2016.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.252 97.9th percentile · FIRST	CISA DEADLINE Mar 24, 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	0.252 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 and should be disconnected if still in use.

Basis: CISA KEV required action

Affected and fixed versions · 4 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	≤ 23.0.0.185 ≤ 11.2.202.637	no fixed version listed	NVD
mac os x	—	no fixed version listed	NVD
chrome os	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
windows 10	1511 1607	no fixed version listed	NVD
windows 8.1	—	no fixed version listed	NVD
windows rt 8.1	—	no fixed version listed	NVD

Sources

Vendor guidance	docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-128	NVD	nvd.nist.gov/vuln/detail/CVE-2016-7855
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2016-8704
Current data	evulnable.com/vulnerability-management/cve/CVE-2016-7855		

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