

CVE-2015-7645

Adobe Flash Player Arbitrary Code Execution Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Ransomware use known

Adobe Flash Player 18.x through 18.0.0.252 and 19.x through 19.0.0.207 on Windows and OS X and 11.x through 11.2.202.535 on Linux allows remote attackers to execute arbitrary code via a crafted SWF file, as exploited in the wild in October 2015.

EVRS 82 / ₁₀₀ Urgent priority	CVSS V3.1 7.8 High · NVD	EPSS 0.653 99.26th 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	Known ransomware campaigns	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.653 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ 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 · 5 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	≥ 18.0.0.160 ≤ 18.0.0.252 19.0.0.185 19.0.0.207 ≤ 11.2.202.535	no fixed version listed	NVD
mac os x	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
evergreen	11.4	no fixed version listed	NVD
opensuse	13.1 13.2	no fixed version listed	NVD
linux enterprise desktop	11 12	no fixed version listed	NVD
linux enterprise workstation extension	12	no fixed version listed	NVD

Sources

Vendor guidance	helpx.adobe.com/security/products/flash-player/apsa15-05.html	NVD	nvd.nist.gov/vuln/detail/CVE-2015-7645
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2015-7548
Current data	evulnable.com/vulnerability-management/cve/CVE-2015-7645		

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