

CVE-2012-0754

Adobe Flash Player Memory Corruption Vulnerability

CISA KEV since Jun 8, 2022

Actively exploited

Public exploit module (Metasploit)

Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

EVRS

82/100

Urgent priority

CVSS V3.1

8.1

High · NVD

EPSS

0.911

99.81st percentile · FIRST

CISA DEADLINE

Jun 22, 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	0.911 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.1	☐ 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	< 10.3.183.15 ≥ 11.0 < 11.1.102.62 < 11.1.111.6 < 11.1.115.6	10.3.183.15 · 11.1.102.62 · 11.1.111.6 · 11.1.115.6	NVD
mac os x	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
solaris	—	no fixed version listed	NVD
android	≥ 2.0 ≤ 3.2 4.0	no fixed version listed	NVD

Sources

Vendor guidance	github.com/advisories/GHSA-p5xj-3764-5mhh	NVD	nvd.nist.gov/vuln/detail/CVE-2012-0754
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2012-0786
Current data	evulnable.com/vulnerability-management/cve/CVE-2012-0754		

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