

CVE-2015-3043

Adobe Flash Player Memory Corruption Vulnerability

CISA KEV since Mar 3, 2022

Actively exploited

Public exploit module (Metasploit)

Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in April 2015, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, and CVE-2015-3042.

EVRs

80/100

Urgent priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.739

99.48th 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	0.739 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ 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 · 6 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	< 11.2.202.457 < 13.0.0.281 ≥ 14.0.0.125 < 17.0.0.169	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
mac os x	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
suse linux enterprise desktop	11.0 12.0	no fixed version listed	NVD
suse linux enterprise workstation extension	12.0	no fixed version listed	NVD
evergreen	11.4	no fixed version listed	NVD
opensuse	13.1 13.2	no fixed version listed	NVD

Sources

Vendor guidance	helpx.adobe.com/security/products/flash-player/apsb15-06.html	NVD	nvd.nist.gov/vuln/detail/CVE-2015-3043
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2015-3124
Current data	evulnable.com/vulnerability-management/cve/CVE-2015-3043		

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