

CVE-2015-5119

Adobe Flash Player Use-After-Free Vulnerability

Exigent

CISA KEV since Mar 3, 2022

Actively exploited

Public exploit module (Metasploit)

Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.296 and 14.x through 18.0.0.194 on Windows and OS X and 11.x through 11.2.202.468 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.

EVRS

87/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.986

99.92nd 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	0.986 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent 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	≥ 13.0.0.182 ≤ 13.0.0296 ≥ 14.0.0.125 ≤ 18.0.0.194 ≤ 11.2.202.468	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
enterprise linux desktop	5.0 6.0	no fixed version listed	NVD
enterprise linux eus	6.6	no fixed version listed	NVD
enterprise linux server	5.0 6.0	no fixed version listed	NVD
enterprise linux server aus	6.6	no fixed version listed	NVD

Sources

Vendor guidance	helpx.adobe.com/security/products/flash-player/apsa15-03.html	NVD	nvd.nist.gov/vuln/detail/CVE-2015-5119
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2015-5134
Current data	evulnable.com/vulnerability-management/cve/CVE-2015-5119		

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