

CVE-2015-0311

Adobe Flash Player Remote Code Execution Vulnerability

CISA KEV since Apr 13, 2022

Actively exploited

Public exploit module (Metasploit)

Unspecified vulnerability in Adobe Flash Player through 13.0.0.262 and 14.x, 15.x, and 16.x through 16.0.0.287 on Windows and OS X and through 11.2.202.438 on Linux allows remote attackers to execute arbitrary code via unknown vectors, as exploited in the wild in January 2015.

EVRS 83/₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.856 99.73rd percentile · FIRST	CISA DEADLINE May 4, 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	0.856 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	$\leq 11.2.202.438$ $\leq 13.0.0.262$ $\geq 14.0.0.125 < 16.0.0.287$	no fixed version listed	NVD
internet explorer	10 11	no fixed version listed	NVD
edge	—	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
linux enterprise desktop	11 12	no fixed version listed	NVD
linux enterprise workstation extension	12	no fixed version listed	NVD

Sources

Vendor guidance	technet.microsoft.com/library/security/2755801	NVD	nvd.nist.gov/vuln/detail/CVE-2015-0311
CISA KEV	cisa.gov/known-exploited-vulnerabilities-catalog	ENISA EUVD	euvd.enisa.europa.eu/vulnerability/EUVD-2015-0324
Current data	evulnable.com/vulnerability-management/cve/CVE-2015-0311		

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