

CVE-2016-4117

Adobe Flash Player Arbitrary Code Execution Vulnerability

Exigent
CISA KEV since Mar 3, 2022
Actively exploited
Ransomware use known
Public exploit module (Metasploit)

Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in May 2016.

EVRS 92 /100 Immediate priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.944 99.85th 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	0.944 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 · 1 more affected product on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	≤ 21.0.0.226	no fixed version listed	NVD
enterprise linux desktop	5.0 6.0	no fixed version listed	NVD
enterprise linux server	5.0 6.0	no fixed version listed	NVD
enterprise linux server from rhui	5.0 6.0	no fixed version listed	NVD
enterprise linux workstation	5.0 6.0	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	12	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-pg3m-fw2-6vrj

Additional guidance helpx.adobe.com/security/products/flash-player/apsa16-02.html

NVD nvd.nist.gov/vuln/detail/CVE-2016-4117

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2016-5118

Current data evaluable.com/vulnerability-management/cve/CVE-2016-4117

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