

CVE-2018-4878

Adobe Flash Player Use-After-Free Vulnerability

CISA KEV since Nov 3, 2021

Actively exploited

Ransomware use known

A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.

EVRS 88 /100 Immediate priority	CVSS V3.1 7.8 High · NVD	EPSS 0.895 99.79th percentile · FIRST	CISA DEADLINE May 3, 2022 KEV since 2021 · 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	0.895 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 7.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch Immediately 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 · 2 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	< 28.0.0.161	no fixed version listed	NVD
macos	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
enterprise linux desktop	6.0	no fixed version listed	NVD
enterprise linux server	6.0	no fixed version listed	NVD
enterprise linux workstation	6.0	no fixed version listed	NVD
windows 10	—	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-2rf4-mpg3-phjw**Additional guidance** helpx.adobe.com/security/products/flash-player/apsb18-03.html**NVD** nvd.nist.gov/vuln/detail/CVE-2018-4878**CISA KEV** cisa.gov/known-exploited-vulnerabilities-catalog**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2018-16663**Current data** evulnable.com/vulnerability-management/cve/CVE-2018-4878

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