

CVE-2016-7892

Adobe Flash Player Use-After-Free Vulnerability

CISA KEV since Mar 25, 2022

Actively exploited

Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the TextField class. Successful exploitation could lead to arbitrary code execution.

EVRS 75 _{/100} Urgent priority	CVSS V3.1 8.8 High · NVD	EPSS 0.188 97.3rd percentile · FIRST	CISA DEADLINE Apr 15, 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	0.188 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 8.8	☐ 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

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player desktop runtime	≤ 23.0.0.207	after 23.0.0.207	NVD
flash player	≤ 23.0.0.207 ≤ 11.2.202.644	after 23.0.0.207 · after 11.2.202.644	NVD
mac os x	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
windows 10	—	no fixed version listed	NVD
windows 8.1	—	no fixed version listed	NVD
chrome os	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD

Sources

Vendor guidance docs.microsoft.com/en-us/security-updates/securitybulletins/2016/ms16-154
NVD nvd.nist.gov/vuln/detail/CVE-2016-7892**ENISA EUVD** euvd.enisa.europa.eu/vulnerability/EUVD-2016-8741**Additional guidance** helpx.adobe.com/security/products/flash-player/apsb16-39.html
CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog
Current data evulnable.com/vulnerability-management/cve/CVE-2016-7892

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