

CVE-2012-0767

Adobe Flash Player Cross-Site Scripting (XSS) Vulnerability

CISA KEV since Jun 8, 2022

Actively exploited

Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Universal XSS (UXSS)," as exploited in the wild in February 2012.

EVRS 75_{/100} Urgent priority	CVSS V3.1 6.1 Medium · NVD	EPSS 0.062 93.5th percentile · FIRST	CISA DEADLINE Jun 22, 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	0.062 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 6.1	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Patch This Cycle No patch reported by the connected remediation source

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	$< 10.3.183.15$ $\geq 11.0 < 11.1.102.62$ $< 11.1.111.6$ $< 11.1.115.6$	$10.3.183.15 \cdot 11.1.102.62$ $11.1.111.6 \cdot 11.1.115.6$	NVD
mac os x	—	no fixed version listed	NVD
linux kernel	—	no fixed version listed	NVD
windows	—	no fixed version listed	NVD
solaris	—	no fixed version listed	NVD
android	$\geq 2.0 \leq 3.2$ 4.0	no fixed version listed	NVD

Sources

NVD nvd.nist.gov/vuln/detail/CVE-2012-0767

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2012-0799

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

Current data evulnable.com/vulnerability-management/cve/CVE-2012-0767

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