

CVE-2015-5123

Adobe Flash Player Use-After-Free Vulnerability

CISA KEV since Apr 13, 2022

Actively exploited

Use-after-free vulnerability in the BitmapData class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.

EVRS 75₁₀₀ Urgent priority	CVSS V3.1 9.8 Critical · NVD	EPSS 0.188 97.3rd 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	0.188 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 · 4 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
flash player	$\geq 11.0 \leq 11.2.202.481$ $\geq 13.0 \leq 13.0.0.302$ $\geq 18.0 \leq 18.0.0.203$	no fixed version listed	NVD
flash player desktop runtime	$\geq 18.0 \leq 18.0.0.203$	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 eus	6.6	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
linux enterprise desktop	11 12	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-6hpg-rw47-66vr

NVD nvd.nist.gov/vuln/detail/CVE-2015-5123

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2015-5138

Additional guidance helpx.adobe.com/security/products/flash-player/apsa15-04.html

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

Current data evulnable.com/vulnerability-management/cve/CVE-2015-5123

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