CVE-2015-5122

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2015-5122
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-07-14 10:59:00 UTC
Updated	2023-05-08 13:29:00 UTC
Description	Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x

Risk And Classification

EPSS: 0.927800000 probability, percentile 0.997570000 (date 2026-04-01)

CISA KEV: Listed on 2022-04-13; due 2022-05-04; ransomware use Unknown

Problem Types: NVD-CWE-Other

CISA Known Exploited Vulnerability

Vendor	Adobe
Product	Flash Player
Name	Adobe Flash Player Use-After-Free Vulnerability
Required Action	The impacted product is end-of-life and should be disconnected if still in use.
Notes	https://nvd.nist.gov/vuln/detail/CVE-2015-5122

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player Desktop Runtime	All	All	All	All
Operating System	Apple	Macos	-	All	All	All

Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Linux	Linux Kernel	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows 8	-	All	All	All
Operating System	Microsoft	Windows 8.0	-	All	All	All
Operating System	Microsoft	Windows 8.0	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Microsoft	Windows 8.1	-	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Opensuse	Evergreen	11.4	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Server Eus	6.6	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation	6.0	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp3	All	All
Operating System	Suse	Linux Enterprise Desktop	11	sp4	All	All
Operating System	Suse	Linux Enterprise Desktop	12	All	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	All	All	All
Operating System	Suse	Linux Enterprise Workstation Extension	12	All	All	All

References

Reference	Source	Link
Adobe Flash Player Use-After-Free Memory Flaw Lets Remote Users Execute Arbitrary Code - SecurityTracker	SECTRACK	www.secur
[security-announce] openSUSE-SU-2015:1267-1: critical: flash-player	SUSE	lists.opensu
Red Hat Customer Portal	REDHAT	rhn.redhat.c
Page not found - Perception Point	MISC	perception-
[security-announce] SUSE-SU-2015:1258-1: critical: Security update for f	SUSE	lists.opensu
Adobe Flash opaqueBackground Use After Free - Exploits Database	EXPLOIT-DB	www.exploi
'[security bulletin] HPSBMU03409 rev.1 - HP Matrix Operating Environment, Multiple Vulnerabilities' - MARC	HP	marc.info
Adobe Flash and Microsoft Windows Vulnerabilities | US-CERT	CERT	www.us-ce
Gentoo Security	GENTOO	security.ge
Adobe Security Bulletin	CONFIRM	helpx.adob
Document Display | HPE Support Center	CONFIRM	h20564.ww
Adobe Security Bulletin	CONFIRM	helpx.adob
CVE-2015-5122 - Second Adobe Flash Zero-Day in HackingTeam Leak « Threat Research | FireEye Inc	MISC	www.fireey
Adobe Flash opaqueBackground Use After Free ≈ Packet Storm	MISC	packetstorm
CVE-2015-5122 Adobe Flash opaqueBackground Use After Free | Rapid7	MISC	www.rapid7
Vulnerability Note VU#338736 - Adobe Flash ActionScript 3 opaqueBackground use-after-free vulnerability	CERT-VN	www.kb.cer
Adobe Flash Player CVE-2015-5122 Use After Free Remote Memory Corruption Vulnerability	BID	www.secur
[security-announce] SUSE-SU-2015:1255-1: critical: Security update for f	SUSE	lists.opensu
Perception Point | Breaking CFI	MISC	perception-
HPSBHF03509	HP	h20564.ww
CVE Program record	CVE.ORG	www.cve.or
NVD vulnerability detail	NVD	nvd.nist.gov
CISA Known Exploited Vulnerabilities catalog	CISA	www.cisa.g

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report