



CVE-2015-3040

Published on: 04/14/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:07 PM UTC

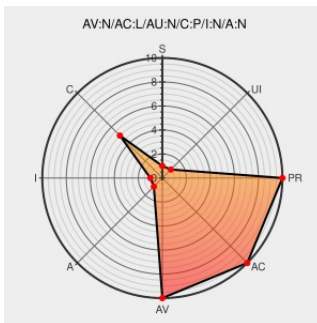
CVE-2015-3040

Source: [Mitre](#)

Source: [NIST](#)

[CVE.ORG](#)

Print: [PDF](#)



Certain versions of [Flash Player](#) from [Adobe](#) contain the following vulnerability:

Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2015-0357.

CVE-2015-3040 has been assigned by psirt@adobe.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Red Hat Customer Portal	Third Party Advisory web.archive.org text/html Inactive Link Not Archived	REDHAT RHSA-2015:0813
[security-announce] openSUSE-SU-2015:0725-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0725
[security-announce] openSUSE-SU-2015:0718-1: important: Security update	Third Party Advisory lists.opensuse.org text/html	SUSE openSUSE-SU-2015:0718
Adobe Flash Player: Multiple vulnerabilities (GLSA 201504-07) — Gentoo security	security.gentoo.org text/html	GENTOO GLSA-201504-07

[security-announce] SUSE-SU-2015:0723-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2015:0723
Adobe Security Bulletin	Patch Vendor Advisory helpx.adobe.com text/html	 CONFIRM helpx.adobe.com/security/products/flash-player/apsb15-06.html
[security-announce] SUSE-SU-2015:0722-1: important: Security update for	Third Party Advisory lists.opensuse.org text/html	 SUSE SUSE-SU-2015:0722
Adobe Flash Player Multiple Bugs Let Remote Users Bypass ASLR, Obtain Potentially Sensitive Information, and Execute Arbitrary Code - SecurityTracker	www.securitytracker.com text/html	 SECTrack 1032105

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Player	14.0.0.125	All	All	All
Application	Adobe	Flash Player	14.0.0.145	All	All	All
Application	Adobe	Flash Player	14.0.0.176	All	All	All
Application	Adobe	Flash Player	14.0.0.179	All	All	All
Application	Adobe	Flash Player	15.0.0.152	All	All	All
Application	Adobe	Flash Player	15.0.0.167	All	All	All
Application	Adobe	Flash Player	15.0.0.189	All	All	All
Application	Adobe	Flash Player	15.0.0.223	All	All	All
Application	Adobe	Flash Player	15.0.0.239	All	All	All
Application	Adobe	Flash Player	15.0.0.246	All	All	All
Application	Adobe	Flash Player	16.0.0.235	All	All	All
Application	Adobe	Flash Player	16.0.0.257	All	All	All
Application	Adobe	Flash Player	16.0.0.287	All	All	All
Application	Adobe	Flash Player	16.0.0.296	All	All	All
Application	Adobe	Flash Player	17.0.0.134	All	All	All
Application	Adobe	Flash Player	14.0.0.125	All	All	All
Application	Adobe	Flash Player	14.0.0.145	All	All	All
Application	Adobe	Flash Player	14.0.0.176	All	All	All
Application	Adobe	Flash Player	14.0.0.179	All	All	All

Application	Adobe	Flash Player	15.0.0.152	All	All	All
Application	Adobe	Flash Player	15.0.0.167	All	All	All
Application	Adobe	Flash Player	15.0.0.189	All	All	All
Application	Adobe	Flash Player	15.0.0.223	All	All	All
Application	Adobe	Flash Player	15.0.0.239	All	All	All
Application	Adobe	Flash Player	15.0.0.246	All	All	All
Application	Adobe	Flash Player	16.0.0.235	All	All	All
Application	Adobe	Flash Player	16.0.0.257	All	All	All
Application	Adobe	Flash Player	16.0.0.287	All	All	All
Application	Adobe	Flash Player	16.0.0.296	All	All	All
Application	Adobe	Flash Player	17.0.0.134	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Application	Adobe	Flash Player	All	All	All	All
Operating System	Apple	Mac Os X	-	All	All	All
Operating System	Apple	Mac Os X	-	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	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Opensuse	Opensuse	13.1	All	All	All
Operating System	Opensuse	Opensuse	13.2	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop Supplementary	6.0	All	All	All
Operating	Redhat	Enterprise Linux Server Supplementary	5.0	All	All	All

System						
Operating System	Redhat	Enterprise Linux Server Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	5.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary Eus	6.6.z	All	All	All
Operating System	Redhat	Enterprise Linux Server Supplementary Eus	6.6.z	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	6.0	All	All	All
Operating System	Redhat	Enterprise Linux Workstation Supplementary	6.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	11.0	sp3	All	All
Operating System	Suse	Suse Linux Enterprise Desktop	12.0	All	All	All
Operating System	Suse	Suse Linux Workstation Extension	12.0	All	All	All
Operating System	Suse	Suse Linux Workstation Extension	12.0	All	All	All
cpe:2.3:a:adobe:flash_player:14.0.0.125:*****:						
cpe:2.3:a:adobe:flash_player:14.0.0.145:*****:						
cpe:2.3:a:adobe:flash_player:14.0.0.176:*****:						
cpe:2.3:a:adobe:flash_player:14.0.0.179:*****:						
cpe:2.3:a:adobe:flash_player:15.0.0.152:*****:						
cpe:2.3:a:adobe:flash_player:15.0.0.167:*****:						
cpe:2.3:a:adobe:flash_player:15.0.0.189:*****:						
cpe:2.3:a:adobe:flash_player:15.0.0.223:*****:						
cpe:2.3:a:adobe:flash_player:15.0.0.239:*****:						
cpe:2.3:a:adobe:flash_player:15.0.0.246:*****:						
cpe:2.3:a:adobe:flash_player:16.0.0.235:*****:						
cpe:2.3:a:adobe:flash_player:16.0.0.257:*****:						

cpe:2.3:a:adobe:flash_player:16.0.0.287:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:16.0.0.296:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:17.0.0.134:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:14.0.0.125:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:14.0.0.145:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:14.0.0.176:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:14.0.0.179:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:15.0.0.152:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:15.0.0.167:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:15.0.0.189:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:15.0.0.223:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:15.0.0.239:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:15.0.0.246:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:16.0.0.235:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:16.0.0.257:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:16.0.0.287:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:16.0.0.296:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:17.0.0.134:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:*:*:*:*:*:
cpe:2.3:a:adobe:flash_player:*:*:*:*:*:
cpe:2.3:o:apple:mac_os_x:-:*:*:*:*:
cpe:2.3:o:apple:mac_os_x:-:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:
cpe:2.3:o:linux:linux_kernel:-:*:*:*:*:
cpe:2.3:o:microsoft:windows:-:*:*:*:*:
cpe:2.3:o:microsoft:windows:-:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:

cpe:2.3:o:opensuse:opensuse:13.1:*:*:*:*:*:
cpe:2.3:o:opensuse:opensuse:13.2:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop_supplementary:5.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop_supplementary:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop_supplementary:5.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_desktop_supplementary:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_supplementary:5.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_supplementary:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_supplementary:5.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_supplementary:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_supplementary_eus:6.6.z:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_server_supplementary_eus:6.6.z:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation_supplementary:6.0:*:*:*:*:*:
cpe:2.3:o:redhat:enterprise_linux_workstation_supplementary:6.0:*:*:*:*:*:
cpe:2.3:o:suse:suse_linux_enterprise_desktop:11.0:sp3:*:*:*:*:*:
cpe:2.3:o:suse:suse_linux_enterprise_desktop:12.0:*:*:*:*:*:
cpe:2.3:o:suse:suse_linux_enterprise_desktop:11.0:sp3:*:*:*:*:*:
cpe:2.3:o:suse:suse_linux_enterprise_desktop:12.0:*:*:*:*:*:
cpe:2.3:o:suse:suse_linux_workstation_extension:12.0:*:*:*:*:*:
cpe:2.3:o:suse:suse_linux_workstation_extension:12.0:*:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)