



CVE-2011-0612

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2011-0612
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-05-16 17:55:00 UTC
Updated	2011-05-25 04:00:00 UTC
Description	Adobe Flash Media Server (FMS) before 3.5.6, and 4.x before 4.0.2, allows remote attackers to cause a denial of service (>

Risk And Classification

Problem Types: CWE-399

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Flash Media Server	2.0	All	All	All
Application	Adobe	Flash Media Server	2.0.1	All	All	All
Application	Adobe	Flash Media Server	2.0.2	All	All	All
Application	Adobe	Flash Media Server	2.0.3	All	All	All
Application	Adobe	Flash Media Server	2.0.4	All	All	All
Application	Adobe	Flash Media Server	2.0.5	All	All	All
Application	Adobe	Flash Media Server	3.0	All	All	All
Application	Adobe	Flash Media Server	3.0.1	All	All	All
Application	Adobe	Flash Media Server	3.0.2	All	All	All
Application	Adobe	Flash Media Server	3.0.3	All	All	All
Application	Adobe	Flash Media Server	3.0.4	All	All	All
Application	Adobe	Flash Media Server	3.0.5	All	All	All
Application	Adobe	Flash Media Server	3.0.6	All	All	All
Application	Adobe	Flash Media Server	3.0.7	All	All	All
Application	Adobe	Flash Media Server	3.5	All	All	All
Application	Adobe	Flash Media Server	3.5.1	All	All	All
Application	Adobe	Flash Media Server	3.5.2	All	All	All

Application	Adobe	Flash Media Server	3.5.3	All	All	All
Application	Adobe	Flash Media Server	3.5.4	All	All	All
Application	Adobe	Flash Media Server	4.0	All	All	All
Application	Adobe	Flash Media Server	4.0.1	All	All	All
Application	Adobe	Flash Media Server	2.0	All	All	All
Application	Adobe	Flash Media Server	2.0.1	All	All	All
Application	Adobe	Flash Media Server	2.0.2	All	All	All
Application	Adobe	Flash Media Server	2.0.3	All	All	All
Application	Adobe	Flash Media Server	2.0.4	All	All	All
Application	Adobe	Flash Media Server	2.0.5	All	All	All
Application	Adobe	Flash Media Server	3.0	All	All	All
Application	Adobe	Flash Media Server	3.0.1	All	All	All
Application	Adobe	Flash Media Server	3.0.2	All	All	All
Application	Adobe	Flash Media Server	3.0.3	All	All	All
Application	Adobe	Flash Media Server	3.0.4	All	All	All
Application	Adobe	Flash Media Server	3.0.5	All	All	All
Application	Adobe	Flash Media Server	3.0.6	All	All	All
Application	Adobe	Flash Media Server	3.0.7	All	All	All
Application	Adobe	Flash Media Server	3.5	All	All	All
Application	Adobe	Flash Media Server	3.5.1	All	All	All
Application	Adobe	Flash Media Server	3.5.2	All	All	All
Application	Adobe	Flash Media Server	3.5.3	All	All	All
Application	Adobe	Flash Media Server	3.5.4	All	All	All
Application	Adobe	Flash Media Server	4.0	All	All	All
Application	Adobe	Flash Media Server	4.0.1	All	All	All
Application	Adobe	Flash Media Server	All	All	All	All

References						
Reference				Source	Link	Tags
Adobe - Security Bulletins: APSB11-11 - Security update available for Adobe Flash Media Server				CONFIRM	www.adobe.com	Patch, Vendor
CVE Program record				CVE.ORG	www.cve.org	canonical
NVD vulnerability detail				NVD	nvd.nist.gov	canonical

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)