



CVE-2016-6934

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

Summary

CVE	CVE-2016-6934
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-15 06:59:00 UTC
Updated	2016-12-23 20:51:00 UTC
Description	Adobe Experience Manager Forms versions 6.2 and earlier, LiveCycle 11.0.1, LiveCycle 10.0.4 have an input validation iss

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Adobe	Experience Manager Forms	All	All	All	All
Application	Adobe	Livecycle	10.0.4	All	All	All
Application	Adobe	Livecycle	11.0.1	All	All	All
Application	Adobe	Livecycle	10.0.4	All	All	All
Application	Adobe	Livecycle	11.0.1	All	All	All

References

Reference	Source
Adobe Experience Manager Forms Input Validation Flaws Let Remote Users Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTF
Adobe Experience Manager and LiveCycle Multiple Cross Site Scripting Vulnerabilities	BID
Adobe Security Bulletin	CONF
CVE Program record	CVE.C
NVD vulnerability detail	NVD

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](#)