



CVE-2017-3109

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

Summary

CVE	CVE-2017-3109
State	PUBLIC
Assigner	psirt@adobe.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-09 06:29:00 UTC
Updated	2017-12-14 14:29:00 UTC
Description	An issue was discovered in Adobe Experience Manager 6.3, 6.2, 6.1, 6.0. Adobe Experience Manager has a reflected cross-site scripting (XSS) vulnerability. An attacker can inject arbitrary HTML and JavaScript into the page. This vulnerability is caused by the lack of output encoding in the <code>renderPage</code> method of the <code>PageRenderer</code> class. The vulnerability is located in the <code>org.apache.sling.scripting.jsp.taglib.JspScriptIncludeTag</code> class. The vulnerability is caused by the lack of output encoding in the <code>renderPage</code> method of the <code>PageRenderer</code> class. The vulnerability is located in the <code>org.apache.sling.scripting.jsp.taglib.JspScriptIncludeTag</code> class.

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	6.0.0	All	All	All
Application	Adobe	Experience Manager	6.1.0	All	All	All
Application	Adobe	Experience Manager	6.2.0	All	All	All
Application	Adobe	Experience Manager	6.3.0	All	All	All
Application	Adobe	Experience Manager	6.0.0	All	All	All
Application	Adobe	Experience Manager	6.1.0	All	All	All
Application	Adobe	Experience Manager	6.2.0	All	All	All
Application	Adobe	Experience Manager	6.3.0	All	All	All

References

Reference
Adobe Experience Manager CVE-2017-3109 Cross Site Scripting Vulnerability
Adobe Security Bulletin
Adobe Experience Manager Flaws Let Remote Users Obtain Potentially Sensitive Information and Conduct Cross-Site Scripting Attacks - SecWiki
CVE Program record
NVD vulnerability detail

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](#)