



CVE-2018-25067

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

Summary

CVE	CVE-2018-25067
State	PUBLIC
Assigner	cna@vuldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-06 21:15:00 UTC
Updated	2023-11-07 02:56:00 UTC
Description	A vulnerability, which was classified as critical, was found in JoomGallery up to 3.3.3. This affects an unknown part of the fil

Risk And Classification

Problem Types: CWE-89

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Joomgallery Project	Joomgallery	All	All	All	All

References

Reference	Source
vuldb.com	MISC
vuldb.com	MISC
Merge pull request #122 from Erfralle/fix-sql-injection-image-ordering · JoomGallery/JoomGallery@dc414ee · GitHub	MISC
Fix SQL Injection Attack Vulnerability via image sorting options by Erfralle · Pull Request #122 · JoomGallery/JoomGallery · GitHub	MISC
Release JoomGallery JUI 3.3.4 · JoomGallery/JoomGallery · GitHub	MISC
CVE Program record	CVE.O
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](#)