



CVE-2022-2846

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

Summary

CVE	CVE-2022-2846
State	PUBLIC
Assigner	cna@vulldb.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-16 19:15:00 UTC
Updated	2023-04-05 18:15:00 UTC
Description	The Calendar Event Multi View WordPress plugin before 1.4.07 does not have any authorisation and CSRF checks in place

Risk And Classification

Problem Types: CWE-79 | CWE-862

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dwbooster	Calendar Event Multi View	All	All	All	All
Application	Dwbooster	Calendar Event Multi View	-	All	All	All

References

Reference	Source
Calendar Event Multi View 1.4.07 Cross Site Scripting ≈ Packet Storm	MISC
CVE-2022-2846 Calendar Event Multi View Plugin cross-site request forgery	MISC
Calendar Event Multi View <= 1.4.06 - Unauthenticated Arbitrary Event Creation to Stored XSS WordPress Security Vulnerability	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

LEGACY: Mostafa Farzaneh

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](#)