



CVE-2022-41996

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

Summary

CVE	CVE-2022-41996
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-10-27 17:15:00 UTC
Updated	2022-11-01 13:54:00 UTC
Description	Cross-Site Request Forgery (CSRF) vulnerability in ThemeFusion Avada premium theme versions <= 7.8.1 on WordPress

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Theme-fusion	Avada	All	All	All	All

References

Reference	Source	Link
theme-fusion.com/documentation-assets/avada/changelog.txt	CONFIRM	theme-fusion.com
WordPress Avada premium theme <= 7.8.1 - Cross-Site Request Forgery (CSRF) vulnerability - Patchstack	CONFIRM	patchstack.com
Avada Website Builder For WordPress & WooCommerce by ThemeFusion	CONFIRM	themeforest.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Dave Jong (Patchstack)

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](#)