



CVE-2022-29429

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

Summary

CVE	CVE-2022-29429
State	PUBLIC
Assigner	audit@patchstack.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-05-17 19:15:00 UTC
Updated	2022-10-07 02:01:00 UTC
Description	Remote Code Execution (RCE) in Alexander Stokmann's Code Snippets Extended plugin <= 1.4.7 on WordPress via Cross

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Code-snippets-extended Project	Code-snippets-extended	All	All	All	All
Application	Code Snippets Extended Project	Code Snippets Extended	All	All	All	All

References

Reference

Code Snippets Extended – WordPress plugin WordPress.org
WordPress Code Snippets Extended plugin <= 1.4.7 - Cross-Site Request Forgery (CSRF) leading to Remote Code Execution (RCE) vulneral
CVE Program record
NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: Vulnerability discovered by Rasi Afeef (Patchstack Alliance)

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](#)