



CVE-2020-11025

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

Summary

CVE	CVE-2020-11025
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-30 22:15:00 UTC
Updated	2020-08-18 15:05:00 UTC
Description	In affected versions of WordPress, a cross-site scripting (XSS) vulnerability in the navigation section of Customizer allows J

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-4677-1 wordpress	DEBIAN	www.d
Authenticated cross-site scripting (XSS) in WordPress Customizer · Advisory · WordPress/wordpress-develop · GitHub	CONFIRM	github.c
Version 5.4.1 WordPress.org	MISC	wordpr
CVE Program record	CVE.ORG	www.cv
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

[730641](#) WordPress Prior to 5.4.1 Multiple Security Vulnerabilities

© [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](#)