

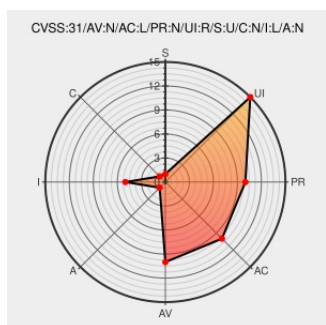


CVE-2020-28040

Published on: 10/30/2020 12:00:00 AM UTC

Last Modified on: 06/29/2022 07:22:00 PM UTC

CVE-2020-28040

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Ubuntu Linux](#) from [Canonical](#) contain the following vulnerability:

WordPress before 5.5.2 allows CSRF attacks that change a theme's background image.

CVE-2020-28040 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **4.3 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	LOW	NONE

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
[SECURITY] [DLA 2429-1] wordpress security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20201103 [SECURITY] [DLA 2429-1] wordpress security update
Debian -- Security Information -- DSA-4784-1 wordpress	www.debian.org	DEBIAN DSA-4784

	Deprecated Link text/html	
[SECURITY] Fedora 32 Update: wordpress-5.5.3-1.fc32 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-b386fac43a
News – WordPress 5.5.2 Security and Maintenance Release – WordPress.org	Release Notes Vendor Advisory wordpress.org text/html	 MISC wordpress.org/news/2020/10/wordpress-5-5-2-security-and-maintenance-release/
[SECURITY] Fedora 33 Update: wordpress-5.5.3-1.fc33 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-a764b11b52
[SECURITY] Fedora 31 Update: wordpress-5.5.3-1.fc31 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	 FEDORA FEDORA-2020-15e15c35da
WordPress 5.2.2 Security Release	Release Notes Vendor Advisory blog.wpscan.com text/html	 MISC blog.wpscan.com/2020/10/30/wordpress-5.5.2-security-release.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

730084 WordPress Prior to 5.5.2 Multiple Vulnerabilities

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Canonical	Ubuntu Linux	16.04	All	All	All
Operating System	Canonical	Ubuntu Linux	18.04	All	All	All
Operating System	Canonical	Ubuntu Linux	20.04	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
cpe:2.3:o:canonical:ubuntu_linux:16.04:***:esm:***:						
cpe:2.3:o:canonical:ubuntu_linux:18.04:***:lts:***:						
cpe:2.3:o:canonical:ubuntu_linux:20.04:***:lts:***:						
cpe:2.3:o:debian:debian_linux:10.0:***:*****:						
cpe:2.3:o:debian:debian_linux:9.0:*****:						

cpe:2.3:a:wordpress:wordpress:.*.*.*.*.*.*.*.*.*.*
cpe:2.3:a:wordpress:wordpress:.*.*.*.*.*.*.*.*.*.*

cpe:2.3:a:wordpress:wordpress:.*.*.*.*.*.*.*.*.*.*
cpe:2.3:a:wordpress:wordpress:.*.*.*.*.*.*.*.*.*.*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? WordPress before 5.5.2 allows CSRF attac... CVE-2020-28040 Link for more: alerts.remotelyrmm.com/CVE-2020-28040	2022-06-29 20:28:30
 @LinInfoSec	Wordpress - CVE-2020-28040: wordpress.org/news/2020/10/w...	2022-06-29 21:03:07

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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](#).

CVE.report and Source URL Uptime Status status.cve.report