



CVE-2020-11027

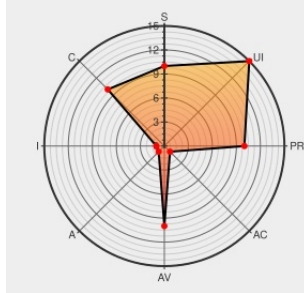
Published on: 04/30/2020 12:00:00 AM UTC

Last Modified on: 06/20/2023 04:15:00 PM UTC

CVE-2020-11027 - advisory for GHSA-ww7v-jg8c-q6jw

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

CVSS:31/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:N/A:N



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

In affected versions of WordPress, a password reset link emailed to a user does not expire upon changing the user password. Access would be needed to the email account of the user by a malicious party for successful execution. This has been patched in version 5.4.1, along with all the previously affected versions via a minor release (5.3.3, 5.2.6, 5.1.5, 5.0.9, 4.9.14, 4.8.13, 4.7.17, 4.6.18, 4.5.21, 4.4.22, 4.3.23, 4.2.27, 4.1.30, 4.0.30, 3.9.31, 3.8.33, 3.7.33).

CVE-2020-11027 has been assigned by [security-advisories@github.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.1 - HIGH**

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

CVSS2 Score: **5.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
WordPress Theme Media 1.0.0 Weak Password	WordPress	MISC

WordPress Theme Medic 1.0.0 Weak Password Recovery Mechanism ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/173034/WordPress-Theme-Medic-1.0.0-Weak-Password-Recovery-Mechanism.html
Debian -- Security Information -- DSA-4677-1 wordpress	Third Party Advisory www.debian.org Deprecated Link text/html	 DEBIAN DSA-4677
[SECURITY] [DLA 2208-1] wordpress security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20200511 [SECURITY] [DLA 2208-1] wordpress security update
Version 5.4.1 WordPress.org	Release Notes Vendor Advisory wordpress.org text/html	 MISC wordpress.org/support/wordpress-version/version-5-4-1/#security-updates
Password reset links invalidation issue in WordPress · Advisory · WordPress/wordpress-develop · GitHub	Third Party Advisory github.com text/html	 CONFIRM github.com/WordPress/wordpress-develop/security/advisories/GHSA-ww7v-jg8c-q6jw

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

730641 WordPress Prior to 5.4.1 Multiple Security Vulnerabilities

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Operating System	Debian	Debian Linux	8.0	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	5.4	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
cpe:2.3:o:debian:debian_linux:10.0:****:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:****:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:****:*:*:						
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:5.4:*:*:*:*:*:
cpe:2.3:a:wordpress:wordpress:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions		
Source	Title	Posted (UTC)
← 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](#)