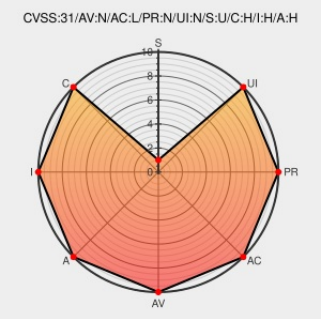
CVE-2020-36724

Published on: Not Yet Published

Last Modified on: 06/13/2023 01:57:00 PM UTC

CVE-2020-36724

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wordable from Wordable contain the following vulnerability:

The Wordable plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.1.1. This is due to the use of a user supplied hashing algorithm passed to the hash_hmac() function and the use of a loose comparison on the hash which allows an attacker to trick the function into thinking it has a valid hash. This makes it possible for unauthenticated attackers to gain administrator privileges.

CVE-2020-36724 has been assigned by security@wordfence.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **wordable** - **Wordable – Export Google Docs to WordPress** version **< 3.1.2**

CVSS3 Score: 9.8 - CRITICAL

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

CVE References

Description	Tags	Link
WordPress Plugins and Themes Vulnerabilities Roundup. – NinTechNet	blog.nintechnet.com text/html	MISC blog.nintechnet.com/wordpress-plugins-and-themes-vulnerabilities-roundup/
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/changeset/2234193/wordable/trunk/wordable.php
Wordable <= 3.1.1 - Authentication Bypass	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/be1ab218-37bd-407a-8cb9-66f761849c21?source=cve

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.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordable	Wordable	All	All	All	All

cpe:2.3:a:wordable:wordable:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

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