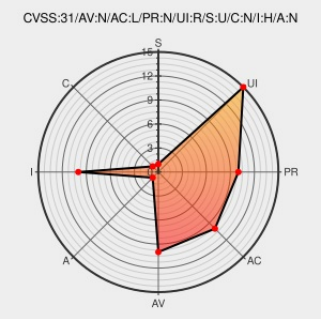
CVE-2023-4277

Published on: Not Yet Published

Last Modified on: 08/15/2023 07:09:00 PM UTC

CVE-2023-4277

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



Certain versions of Realia from Pragmaticmates contain the following vulnerability:

The Realia plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.4.0. This is due to missing nonce validation on the 'process_change_profile_form' function. This makes it possible for unauthenticated attackers to change user email via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.

CVE-2023-4277 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **pragmaticmates** - **Realia** version **<= 1.4.0**

CVSS3 Score: 6.5 - MEDIUM

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

CVE References

Description	Tags	Link
Realia <= 1.4.0 - Cross-Site Request Forgery to User Email Change	www.wordfence.com text/html	MISC www.wordfence.com/threat-intel/vulnerabilities/id/06f33e18-0bdd-4c56-a8df-fc1969b9ecf8?source=cve
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/realia/tags/1.4.0/includes/post-types/class-realia-post-type-user.php#L112

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	Pragmaticmates	Realia	All	All	All	All

cpe:2.3:a:pragmaticmates:realia:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→