

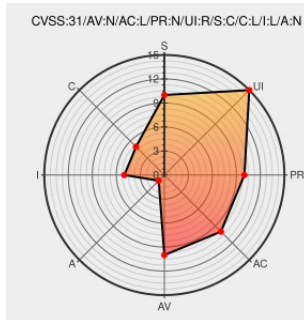


CVE-2021-24299

Published on: 05/17/2021 12:00:00 AM UTC

Last Modified on: 05/24/2021 07:16:00 PM UTC

CVE-2021-24299

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

Certain versions of [Redi Restaurant Reservation](#) from [Catzsoft](#) contain the following vulnerability:

The ReDi Restaurant Reservation WordPress plugin before 21.0426 provides the functionality to let users make restaurant reservations. These reservations are stored and can be listed on an 'Upcoming' page provided by the plugin. An unauthenticated user can fill in the form to make a restaurant reservation. The form to make a restaurant

reservation field called 'Comment' does not use proper input validation and can be used to store XSS payloads. The XSS payloads will be executed when the plugin user goes to the 'Upcoming' page, which is an external website <https://upcoming.reservationdiary.eu/> loaded in an iframe, and the stored reservation with XSS payload is loaded.

CVE-2021-24299 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Reservation Diary - ReDi Restaurant Reservation** version < 21.0426

CVSS3 Score: **6.1 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	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
WordPress ReDi Restaurant Reservation 21.0307 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	 MISC packetstormsecurity.com/files/162756/WordPress-ReDi-Restaurant-Reservation-21.0307-Cross-Site-Scripting.html
Attention Required! Cloudflare	wpscan.com text/html Inactive Link Not Archived	 CONFIRM wpscan.com/vulnerability/fd6ce00b-8c5f-4180-b648-f47b37303670

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	Catzsoft	Redi Restaurant Reservation	All	All	All	All
cpe:2.3:a:catzsoft:redi_restaurant_reservation:*:*:*:*:wordpress:*:*						

Discovery Credit

Bastijn Ouwendijk

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-24299 : The ReDi Restaurant Reservation WordPress plugin before 21.0426 provides the functionality to let... twitter.com/i/web/status/1...	2021-05-17 16:55:43
 @LinInfoSec	Wordpress - CVE-2021-24299: wpscan.com/vulnerability/...	2021-05-17 18:35:53
 /r/netcve	CVE-2021-24299	2021-05-17 17:41:43

[← 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](#)