



CVE-2021-38346

Published on: 10/14/2021 12:00:00 AM UTC

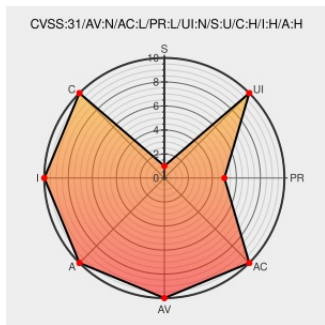
Last Modified on: 10/18/2021 07:20:00 PM UTC

CVE-2021-38346

Source: Mitre

Source: Nist

Print: PDF



Certain versions of **Brizy-page Builder** from **Brizy** contain the following vulnerability:

The Brizy Page Builder plugin <= 2.3.11 for WordPress allowed authenticated users to upload executable files to a location of their choice using the `brizy_create_block_screenshot` AJAX action. The file would be named using the `id` parameter, which could be prepended with `../` to perform directory traversal, and the file contents were populated via the `ibsf` parameter, which would be base64-decoded and written to the file. While the plugin added a `.jpg` extension to all uploaded filenames, a double extension attack was still possible, e.g. a file named `shell.php` would be saved as `shell.php.jpg`, and would be executable on a number of common configurations.

CVE-2021-38346 has been assigned by security@wordfence.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Brizy.io - Brizy - Page Builder** version <= 2.3.11

CVSS3 Score: **8.8 - HIGH**

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

CVSS2 Score: **6.5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Multiple Vulnerabilities in Brizy Page Builder Plugin Allow Site Takeover	www.wordfence.com text/html	 MISC www.wordfence.com/blog/2021/10/multiple-vulnerabilities-in-brizy-page-builder-plugin-allow-site-takeover/

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	Brizy	Brizy-page Builder	All	All	All	All

```
cpe:2.3:a:brizy:brizy-page_builder:*:*:*:wordpress:*:*:
```

Discovery Credit

Ramuel Gall, Wordfence

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2021-38346 : The Brizy Page Builder plugin <= 2.3.11 for WordPress allowed authenticated users to upload execut... twitter.com/i/web/status/1...	2021-10-14 16:06:05

[← Previous ID](#)

[Next ID →](#)

© CVE.report 2021   |

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