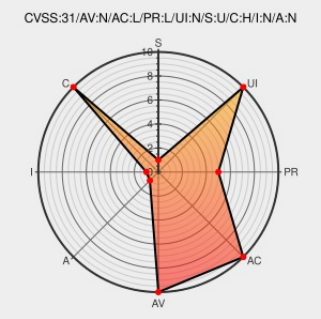
CVE-2021-39351

Published on: 10/06/2021 12:00:00 AM UTC

Last Modified on: 10/14/2021 02:53:00 PM UTC

CVE-2021-39351

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



Certain versions of Wp Bannerize from Wp Bannerize Project contain the following vulnerability:

The WP Bannerize WordPress plugin is vulnerable to authenticated SQL injection via the id parameter found in the ~/Classes/wpBannerizeAdmin.php file which allows attackers to exfiltrate sensitive information from vulnerable sites. This issue affects versions 2.0.0 - 4.0.2.

CVE-2021-39351 has been assigned by security@wordfence.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **WP Bannerize** - **WP Bannerize** version **= 4.0.2**

CVSS3 Score: 6.5 - MEDIUM

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

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
Vulnerability Advisories -	www.wordfence.com	MISC www.wordfence.com/vulnerability-advisories/#CVE-2021-39351

Wordfence	text/html	
403 Forbidden	plugins.trac.wordpress.org text/html Inactive Link Not Archived	MISC plugins.trac.wordpress.org/browser/wp-bannerize/trunk/Classes/wpBannerizeAdmin.php#L1681

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	Wp Bannerize Project	Wp Bannerize	All	All	All	All

cpe:2.3:a:wp_bannerize_project:wp_bannerize:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Margaux DABERT from Intrinsec

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-39351 : The WP Bannerize WordPress plugin is vulnerable to authenticated SQL injection via the id paramete… twitter.com/i/web/status/1…	2021-10-06 16:05:10
@LinInfoSec	Php - CVE-2021-39351: plugins.trac.wordpress.org/browser/wp-ban…	2021-10-06 19:15:44

← 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 registred 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