



CVE-2020-36714

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-36714
State	PUBLIC
Assigner	security@wordfence.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-20 08:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	The Brizy plugin for WordPress is vulnerable to authorization bypass due to a incorrect capability check on the is_administr

Risk And Classification

Problem Types: CWE-863

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Brizy	Brizy-page Builder	All	All	All	All

References

Reference	Source	Link	Tags
Brizy < 1.0.126 - Authorization Bypass to Settings Updates	MISC	www.wordfence.com	
WordPress Brizy Page Builder plugin fixed critical vulnerabilities. – NinTechNet	MISC	blog.nintech.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)