



CVE-2020-36731

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

Summary

CVE	CVE-2020-36731
State	PUBLIC
Assigner	security@wordfence.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-06-07 02:15:00 UTC
Updated	2023-11-07 03:22:00 UTC
Description	The Flexible Checkout Fields for WooCommerce plugin for WordPress is vulnerable to Unauthenticated Arbitrary Plugin Se

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpdesk	Flexible Checkout Fields For Woocommerce	All	All	All	All

References

Reference	Source	Link
Flexible Checkout Fields for WooCommerce <= 2.3.1 - Unauthenticated Arbitrary Plugin Settings Update	MISC	www.wordfence.com
Site Takeover Campaign Exploits Multiple Zero-Day Vulnerabilities	MISC	www.wordfence.com
Zero-day vulnerability fixed in WordPress Flexible Checkout Fields for WooCommerce plugin. – NinTechNet	MISC	blog.nintech.net
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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