



CVE-2022-29416

Published on: Not Yet Published

Last Modified on: 02/13/2023 02:37:00 PM UTC

CVE-2022-29416

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

Certain versions of [Afterpay Gateway For Woocommerce](#) from [Afterpay](#) contain the following vulnerability:

Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Afterpay Gateway for WooCommerce <= 3.5.0 versions.

CVE-2022-29416 has been assigned by audit@patchstack.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **Afterpay - Afterpay Gateway for WooCommerce** version = n/a

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

CVE References

Description	Tags	Link
WordPress Afterpay Gateway for WooCommerce plugin <= 3.5.0 - Unauth. Reflected Cross-Site Scripting (XSS) vulnerability - Patchstack	patchstack.com text/html	MISC patchstack.com/database/vulnerability/afterpay-gateway-for-woocommerce/wordpress-afterpay-gateway-for-woocommerce-plugin-3-5-0-unauth-reflected-cross-site-scripting-xss-vulnerability?_s_id=cve

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

Exploit/POC from Github

Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Afterpay Gateway for WooCommerce <= 3.5.0 versions. CVE...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Afterpay	Afterpay Gateway For Woocommerce	All	All	All	All
cpe:2.3:a:afterpay:afterpay_gateway_for_woocommerce:*:*:*:*:wordpress:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @CVEreport	CVE-2022-29416 : Unauth. Reflected Cross-Site Scripting #XSS vulnerability in Afterpay Gateway for WooCommerce <=... twitter.com/i/web/status/1...	2023-02-06 13:06:33
 @threatmeter	CVE-2022-29416 Afterpay Gateway for WooCommerce Plugin up to 3.5.0 on WordPress cross site scripting A vulnerabil... twitter.com/i/web/status/1...	2023-02-06 16:51:29
 /r/netcve	CVE-2022-29416	2023-02-06 14:40:56

[← 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](#)