



CVE-2022-4017

Published on: Not Yet Published

Last Modified on: 01/31/2023 06:53:00 PM UTC

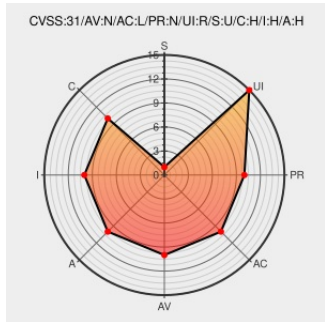
CVE-2022-4017

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Booster Elite WooCommerce](#) from [Booster](#) contain the following vulnerability:

The [Booster for WooCommerce WordPress](#) plugin before 6.0.1, [Booster Plus for WooCommerce WordPress](#) plugin before 6.0.1, [Booster Elite for WooCommerce WordPress](#) plugin before 6.0.1 have either flawed CSRF checks or are missing them completely in numerous places, allowing attackers to make logged in users perform unwanted actions via CSRF attacks

CVE-2022-4017 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **Unknown** - [Booster for WooCommerce](#) version = 0

Affected Vendor/Software: **Unknown** - [Booster Plus for WooCommerce](#) version = 0

Affected Vendor/Software: **Unknown** - [Booster Elite for WooCommerce](#) version = 0

CVSS3 Score: **8.8 - HIGH**

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

CVE References

Description	Tags	Link
Booster for WooCommerce - Multiple CSRF WordPress Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	wpscan.com/vulnerability/609072d0-9bb9-4fe0-9626-7e4a334ca3a4

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

The Booster for WooCommerce WordPress plugin before 6.0.1, Booster Plus for WooCommerce WordPress plugin before 6.0.1...

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Booster	Booster Elite Woocommerce	All	All	All	All
Application	Booster	Booster For Woocommerce	All	All	All	All
Application	Booster	Booster Plus Woocommerce	All	All	All	All



cpe:2.3:a:booster:booster_elite_woocommerce:*:*:*:*:wordpress:*:*:

cpe:2.3:a:booster:booster_for_woocommerce:*:*:*:*:wordpress:*:*:

cpe:2.3:a:booster:booster_plus_woocommerce:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @m0rb	CVE-2022-4017RUCK twitter.com/NotifyNYC/stat...	2022-04-06 18:39:44
 @CVEreport	CVE-2022-4017 : The Booster for WooCommerce WordPress plugin before 6.0.1, Booster Plus for WooCommerce WordPress p... twitter.com/i/web/status/1...	2023-01-23 15:04:34

[← 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](#)