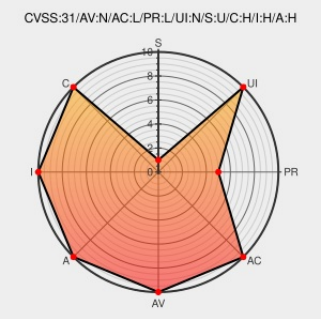
CVE-2021-24190

Published on: 05/14/2021 12:00:00 AM UTC

Last Modified on: 07/30/2022 12:36:00 PM UTC

CVE-2021-24190

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



Certain versions of Conditional Marketing Mailer from Wp-buy contain the following vulnerability:

Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the WooCommerce Conditional Marketing Mailer WordPress plugin before 1.5.2, to install any plugin (including a specific version) from the WordPress repository, as well as activate arbitrary plugin from then blog, which helps attackers install vulnerable plugins and could lead to more critical vulnerabilities like RCE.

CVE-2021-24190 has been assigned by contact@wpscan.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **wp-buy** - **WooCommerce Conditional Marketing Mailer** version **< 1.5.2**

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 6.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Multiple WP-Buy Plugins - Arbitrary Plugin Installation/Activation via Low Privilege User Security Vulnerability	web.archive.org text/html Inactive Link Not Archived	CONFIRM wpscan.com/vulnerability/74889e29-5349-43d1-baf5-1622493be90c

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-buy	Conditional Marketing Mailer	All	All	All	All

cpe:2.3:a:wp-buy:conditional_marketing_mailer:*:*:*:*:*:wordpress:*:*:

Discovery Credit

Bugbang

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-24190 : Low privileged users can use the AJAX action 'cp_plugins_do_button_job_later_callback' in the WooC… twitter.com/i/web/status/1…	2021-05-14 11:47:34
/r/netcve	CVE-2021-24190	2021-05-14 12:41:06

← Previous ID

Next ID→