

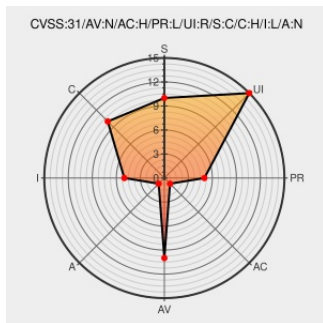


CVE-2020-5293

Published on: 04/20/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:02 PM UTC

CVE-2020-5293 - advisory for GHSA-cvjj-grfv-f56w

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

Certain versions of [Prestashop](#) from [Prestashop](#) contain the following vulnerability:

In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there are improper access controls on product page with combinations, attachments and specific prices. The problem is fixed in 1.7.6.5.

CVE-2020-5293 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **PrestaShop** - **PrestaShop** version $\geq 1.7.0.0$, $< 1.7.6.5$

CVSS3 Score: **6.5 - MEDIUM**

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

CVSS2 Score: **6.4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Improper access control on product page with combinations.	Patch Third Party Advisory	CONFIRM github.com/PrestaShop/PrestaShop/security/advisories/GHSA-cvjj-grfv-f56w

github.com
text/html

```
Patch
Third Party Advisory
github.com
text/html
```

github.com/PrestaShop/PrestaShop/commit/f9f442c87755908e23a6bcba8c443cde

comment@cve.report.

Known Affected Configurations (CPE V2.3)

```
cpe:2.3:a:prestashop:prestashop:*:*:*:*:*:*:*:
```

[← Previous ID](#)

Next ID→

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.report and Source URL Uptime Status status.cve.report