

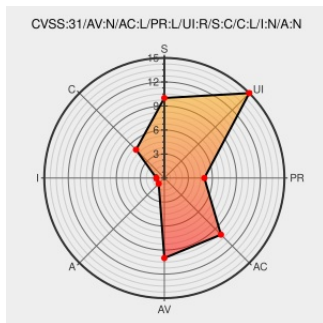


CVE-2020-5285

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

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

CVE-2020-5285 - advisory for GHSA-j3r6-33hf-m8wh

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

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

In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is a reflected XSS with `back` parameter. The problem is fixed in 1.7.6.5

CVE-2020-5285 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: **PrestaShop** - **PrestaShop** version $\geq 1.7.6.0$, $< 1.7.6.5$

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

CVSS2 Score: **4.3 - MEDIUM**

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

CVE References

Description	Tags	Link
Reflected XSS with back parameter - Advisory -	Patch Third Party Advisory	CONFIRM github.com/PrestaShop/PrestaShop/security/advisories/GHSA-j3r6-m8wh

parameter: Advisory

PrestaShop/PrestaShop · GitHub

Third Party Advisory

github.com

text/html

Merge pull request from GHSA-j3r6-33hf-m8wh · PrestaShop/PrestaShop@b6aea15 · GitHub

Patch

Third Party Advisory

github.com

text/html

MISC

github.com/PrestaShop/PrestaShop/commit/b6aea152988d81e1586f1c03f2e72c9

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Prestashop	Prestashop	All	All	All	All
Application	Prestashop	Prestashop	All	All	All	All

cpe:2.3:a:prestashop:prestashop:*****:.*

cpe:2.3:a:prestashop:prestashop:*****:.*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →