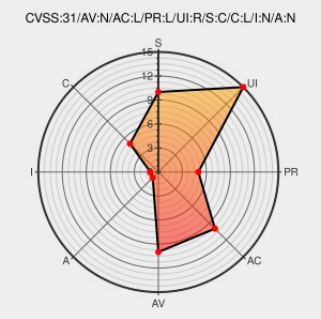
CVE-2020-5276

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

Last Modified on: 03/23/2021 11:24:04 PM UTC

CVE-2020-5276 - advisory for GHSA-q6pr-42v5-v97q

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



Certain versions of Prestashop from Prestashop contain the following vulnerability:

In PrestaShop between versions 1.7.1.0 and 1.7.6.5, there is a reflected XSS on AdminCarts page with `cartBox` parameter The problem is fixed in 1.7.6.5

CVE-2020-5276 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **PrestaShop** - **PrestaShop** version **>= 1.7.1.0, < 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 on AdminCarts page · Advisory ·	Patch Third Party Advisory	CONFIRM github.com/PrestaShop/PrestaShop/security/advisories/GHSA-q6pr-v97q

PrestaShop/PrestaShop · GitHub	github.com text/html	
Merge pull request from GHSA-q6pr-42v5-v97q · PrestaShop/PrestaShop@6838d21 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/PrestaShop/PrestaShop/commit/6838d21850e7227fb8afbf568cb0386

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→