



CVE-2020-5273

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2020-5273
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-04-16 22:15:00 UTC
Updated	2020-04-22 18:36:00 UTC
Description	In PrestaShop module ps_linklist versions before 3.1.0, there is a stored XSS when using custom URLs. The problem is fix

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link	Tags
Merge pull request from GHSA-cx2r-mf6x-55rx · PrestaShop/ps_linklist@83e6e0b · GitHub	MISC	github.com	Patch, Third Party
Stored XSS with custom URLs · Advisory · PrestaShop/ps_linklist · GitHub	CONFIRM	github.com	Third Party Advisor
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)