



CVE-2019-12313

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

Summary

CVE	CVE-2019-12313
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-05-24 14:29:00 UTC
Updated	2019-05-28 15:05:00 UTC
Description	XSS exists in Shave before 2.5.3 because output encoding is mishandled during the overwrite of an HTML element.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Dollarshaveclub	Shave	All	All	All	All
Application	Dollarshaveclub	Shave	All	All	All	All

References

Reference	Source	Link	Tags
[version] patch; @digitalcraft createTextNode() ???? (#146) · dollarshaveclub/shave@da7371b · GitHub	MISC	github.com	Pa
Overview	MISC	www.npmjs.com	Th
Comparing 852b537...da7371b · dollarshaveclub/shave · GitHub	MISC	github.com	Pa
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[981782](#) Nodejs (npm) Security Update for shave (GHSA-gh4g-3gm9-5wrq)

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, 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](#).

Free CVE JSON API cve.report/api

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