



CVE-2015-9413

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

Summary

CVE	CVE-2015-9413
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-26 00:15:00 UTC
Updated	2019-09-27 12:35:00 UTC
Description	The eshop plugin through 6.3.13 for WordPress has CSRF with resultant XSS via the wp-admin/admin.php?page=eshop-d

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Eshop Project	Eshop	All	All	All	All

References

Reference	Source	Link	Tags
eShop – WordPress plugin WordPress.org	MISC	wordpress.org	Product, Third Party Advisory
eShop - Reflected Cross-Site Scripting (XSS) & CSRF	MISC	wpvulndb.com	Exploit, Third Party Advisory
WordPress eShop 6.3.13 Cross Site Scripting ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third Party Advisory, VDB E
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](#).

Free CVE JSON API cve.report/api

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