



CVE-2019-12934

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

Summary

CVE	CVE-2019-12934
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-07-20 00:15:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	An issue was discovered in the wp-code-highlightjs plugin through 0.6.2 for WordPress. wp-admin/options-general.php?page=wp-code-highlightjs

Risk And Classification

Problem Types: CWE-352 | CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wp-code-highlightjs Project	Wp-code-highlightjs	All	All	All	All

References

Reference	Source	Link
WordPress › WP Code Highlight.js « WordPress Plugins	MISC	wordpress.org/plugins/wp-code-highlightjs/
CVE-2019-12934 – wp-code-highlightjs WordPress Plugin CSRF leads to blog-wide injected script/HTML – ZeroAuth	MISC	zeroauth.io/blog/cve-2019-12934-wp-code-highlightjs-wordpress-plugin-csrf-leads-to-blog-wide-injected-script/html-zeroauth/
WordPress 'wp-code-highlightjs' Plugin CVE-2019-12934 Cross Site Request Forgery Vulnerability	BID	www.exploit-db.com/exploits/45888/">www.exploit-db.com/exploits/45888/
CVE Program record	CVE.ORG	www.cve.org/CVERecord?id=CVE-2019-12934">www.cve.org/CVERecord?id=CVE-2019-12934
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2019-12934">nvd.nist.gov/vuln/detail/CVE-2019-12934

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