CVE-2015-5057

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2015-5057
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-18 18:29:00 UTC
Updated	2020-03-14 00:15:00 UTC
Description	Cross-site scripting (XSS) vulnerability exists in the Wordpress admin panel when the Broken Link Checker plugin before 1.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Broken Link Checker Project	Broken Link Checker	All	All	All	All

References

Reference
WordPress › Broken Link Checker « WordPress Plugins
Broken Link Checker <= 1.10.8 - Unauthenticated Stored XSS
WordPress Broken Link Checker Plugin CVE-2015-5057 HTML Injection Vulnerability
oss-security - Re: CVE Request for Wordpress-Plugin Broken Link Checker v1.10.8: Persistent XSS in admin panel enabled by modified head
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

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