CVE-2018-20150

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

Summary

CVE	CVE-2018-20150
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-12-14 20:29:00 UTC
Updated	2019-03-04 14:21:00 UTC
Description	In WordPress before 4.9.9 and 5.x before 5.0.1, crafted URLs could trigger XSS for certain use cases involving plugins.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Link	Tags
Debian -- Security Information -- DSA-4401-1 wordpress	DEBIAN	www.debian.org	Third Party Adviso
Version 4.9.9 | WordPress.org	MISC	codex.wordpress.org	Product, Vendor A
WordPress Prior to 5.0.1 Multiple Security Vulnerabilities	BID	www.securityfocus.com	Third Party Adviso
WordPress 5.0.1 Security Release	MISC	wordpress.org	Release Notes, Ve
[SECURITY] [DLA 1673-1] wordpress security update	MLIST	lists.debian.org	Mailing List, Third
Version 5.0.1 | WordPress.org	MISC	wordpress.org	Release Notes, Ve
WordPress plugs bug that led to Google indexing some user passwords | ZDNet	MISC	www.zdnet.com	Press/Media Cove
KSES: Make the URI attributes DRY. · WordPress/WordPress@fb3c6ea · GitHub	MISC	github.com	Patch, Third Party
WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins	MISC	wpvulndb.com	Vendor Advisory

WordPress <= 5.0 - Cross-Site Scripting (XSS) that could affect plugins	MISC	wpvulndb.com	Vendor Advisory
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.

Free CVE JSON API cve.report/api

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