CVE-2019-9787

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

Summary

CVE	CVE-2019-9787
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-14 16:29:00 UTC
Updated	2019-03-31 22:29:00 UTC
Description	WordPress before 5.1.1 does not properly filter comment content, leading to Remote Code Execution by unauthenticated u

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Link	Tags
WordPress 3.9-5.1 - Comment Cross-Site Scripting (XSS)	MISC	wpvulndb.com	
Comments: Improve comment content filtering. · WordPress/WordPress@0292de6 · GitHub	MISC	github.com	Patch,
WordPress 5.1 CSRF to Remote Code Execution	MISC	blog.ripstech.com	Exploit,
Debian -- Security Information -- DSA-4677-1 wordpress	DEBIAN	www.debian.org	
Version 5.1.1 | WordPress.org	MISC	wordpress.org	Release
WordPress CVE-2019-9787 Remote Code Execution Vulnerability	BID	www.securityfocus.com	Third P
News – WordPress 5.1.1 Security and Maintenance Release – WordPress.org	MISC	wordpress.org	Release
[SECURITY] [DLA 1742-1] wordpress security update	MLIST	lists.debian.org	
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

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**