CVE-2019-16780

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

Summary

CVE	CVE-2019-16780
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-12-26 17:15:00 UTC
Updated	2022-11-23 20:12:00 UTC
Description	WordPress users with lower privileges (like contributors) can inject JavaScript code in the block editor using a specific paylo

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	10.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	3.7	-	All	All
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	3.7	-	All	All

References

Reference	Source	Link
Prevent stored XSS in the block editor. · WordPress/wordpress-develop@505dd6a · GitHub	MISC	github.com
HackerOne	MISC	hackerone.co
Stored cross-site scripting (XSS) in WordPress block editor · Advisory · WordPress/wordpress-develop · GitHub	CONFIRM	github.com
Debian -- Security Information -- DSA-4677-1 wordpress	DEBIAN	www.debian.c
WordPress <= 5.3 - Stored XSS via Block Editor Content	MISC	wpvulndb.com
News – WordPress 5.3.1 Security and Maintenance Release – WordPress.org	MISC	wordpress.org
Debian -- Security Information -- DSA-4599-1 wordpress	DEBIAN	www.debian.c
Bugtraq: [SECURITY] [DSA 4599-1] wordpress security update	BUGTRAQ	seclists.org

CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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