CVE-2020-4046

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

Summary

CVE	CVE-2020-4046
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-06-12 16:15:00 UTC
Updated	2023-11-07 03:23:00 UTC
Description	In affected versions of WordPress, users with low privileges (like contributors and authors) can use the embed block in a ce

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	Fedoraproject	Fedora	31	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Application	Wordpress	Wordpress	All	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 32 Update: wordpress-5.4.2-1.fc32 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
[SECURITY] Fedora 31 Update: wordpress-5.4.2-1.fc31 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or
News – WordPress 5.4.2 Security and Maintenance Release – WordPress.org	MISC	wordpress.org
[SECURITY] Fedora 31 Update: wordpress-5.4.2-1.fc31 - package-announce - Fedora Mailing-Lists	FEDORA	lists.fedoraproject.or
WordPress: Authenticated XSS through embed block · Advisory · WordPress/wordpress-develop · GitHub	CONFIRM	github.com
Debian -- Security Information -- DSA-4709-1 wordpress	DEBIAN	www.debian.org
[SECURITY] [DLA 2269-1] wordpress security update	MLIST	lists.debian.org
[SECURITY] Fedora 32 Update: wordpress-5.4.2-1.fc32 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.or

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.