CVE-2015-3440

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

Summary

CVE	CVE-2015-3440
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-03 14:59:00 UTC
Updated	2016-12-06 03:01:00 UTC
Description	Cross-site scripting (XSS) vulnerability in wp-includes/wp-db.php in WordPress before 4.2.1 allows remote attackers to inje

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	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Lin
WordPress › WordPress 4.2.1 Security Release	CONFIRM	wo
121320	OSVDB	osv
Version 4.2.1 « WordPress Codex	CONFIRM	coc
WordPress Comment Section HTML Injection Vulnerability	BID	ww
WordPress <= 4.2 - Stored XSS - Exploits Database	EXPLOIT-DB	ww
Changeset 32299 – WordPress Trac	CONFIRM	cor
WordPress 4.2 Cross Site Scripting ≈ Packet Storm	MISC	pac
Debian -- Security Information -- DSA-3250-1 wordpress	DEBIAN	ww
[SECURITY] Fedora 21 Update: wordpress-4.2.2-1.fc21	FEDORA	lists

WordPress Input Validation Flaw in Processing Large Comments Permits Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	ww
Full Disclosure: WordPress 4.2 stored XSS	FULLDISC	sec
[SECURITY] Fedora 22 Update: wordpress-4.2.1-1.fc22	FEDORA	lists
[SECURITY] Fedora 20 Update: wordpress-4.2.2-1.fc20	FEDORA	lists
WordPress <= 4.2 - Unauthenticated Stored Cross-Site Scripting (XSS)	MISC	wp
Klikki Oy - WordPress 4.2 Stored XSS	MISC	klik
CVE Program record	CVE.ORG	ww
NVD vulnerability detail	NVD	nvd

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**