CVE-2015-5622

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

Summary

CVE	CVE-2015-5622
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-08-03 14:59:00 UTC
Updated	2017-11-04 01:29:00 UTC
Description	Cross-site scripting (XSS) vulnerability in WordPress before 4.2.3 allows remote authenticated users to inject arbitrary web

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	8.0	All	All	All
Application	Wordpress	Wordpress	All	All	All	All

References

Reference	Source	Link
Debian -- Security Information -- DSA-3332-1 wordpress	DEBIAN	www.debian.org
Debian -- Security Information -- DSA-3383-1 wordpress	DEBIAN	www.debian.org
Klikki Oy - WordPress < 4.2.3 Stored XSS	MISC	klikki.fi
WordPress › WordPress 4.2.3 Security and Maintenance Release	CONFIRM	wordpress.org
WordPress <= 4.2.2 - Authenticated Stored Cross-Site Scripting (XSS)	MISC	wpvulndb.com
Debian -- Security Information -- DSA-3328-1 wordpress	DEBIAN	www.debian.org
Malformed Request	BID	www.securityfocus.cor
WordPress Input Validation Flaws Let Remote Conduct Cross-Site Scripting Attacks - SecurityTracker	SECTRACK	www.securitytracker.c
Changeset 33359 – WordPress Trac	CONFIRM	core.trac.wordpress.or
oss-security - Re: CVE request: WordPress 4.2.2 and earlier cross-site scripting vulnerability	MLIST	openwall.com
Version 4.2.3 « WordPress Codex	CONFIRM	codex.wordpress.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.

© CVE.report 2026 |
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

Free CVE JSON API cve.report/api

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