CVE-2014-9443

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

Summary

CVE	CVE-2014-9443
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-01-02 19:59:00 UTC
Updated	2015-01-05 21:16:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the Relevanssi plugin before 3.3.8 for WordPress allows remote attackers to injec

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Relevanssi	Relevanssi	3.3.7.1	All	All	All
Application	Relevanssi	Relevanssi	3.3.7.1	All	All	All

References

Reference	Source	Link	Tags
Security Advisory SA61744 - WordPress Relevanssi Plugin Cross-Site Scripting Vulnerability - Secunia	SECUNIA	secunia.com	
WordPress › Relevanssi - A Better Search « WordPress Plugins	CONFIRM	wordpress.org	Patch
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

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