



CVE-2017-1000038

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2017-1000038
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-07-17 13:18:00 UTC
Updated	2017-07-20 18:54:00 UTC
Description	WordPress plugin Relevanssi version 3.5.7.1 is vulnerable to stored XSS resulting in attacker being able to execute JavaSc

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Relevanssi	Relevanssi	3.5.7.1	All	All	All
Application	Relevanssi	Relevanssi	3.5.7.1	All	All	All

References

Reference	Source	Li
Stored XSS in Relevanssi could allow an unauthenticated attacker to do almost anything an admin can do – dxw advisories	MISC	se
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

No vendor comments have been submitted for this CVE.

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

CVE, CWE, and OVAL are registered 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