



CVE-2017-12777

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

Summary

CVE	CVE-2017-12777
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-08-09 21:29:00 UTC
Updated	2017-08-30 01:29:00 UTC
Description	Cross-Site Scripting (XSS) exists in NexusPHP version v1.5 via some parameter to usersearch.php.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Nexusphp Project	Nexusphp	1.5	All	All	All
Application	Nexusphp Project	Nexusphp	1.5	All	All	All

References

Reference	Source	Link	Tags
lu4n.com/cve/4.txt	MISC	lu4n.com	Third Party Advisory
Site not found · GitHub Pages	MISC	www.d4rksec.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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