



CVE-2014-4717

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

Summary

CVE	CVE-2014-4717
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-03 14:55:00 UTC
Updated	2022-11-15 17:34:00 UTC
Description	Multiple cross-site request forgery (CSRF) vulnerabilities in the Simple Share Buttons Adder plugin before 4.5 for WordPress

Risk And Classification

Problem Types: CWE-352

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Davidsneal	Simple Share Buttons Adder	1.0	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.1	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.2	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.3	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.4	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.5	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.6	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.7	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.8	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	1.9	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	2.0	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	2.1	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	2.2	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	2.3	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	2.4	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	2.5	All	All	All
Application	Davidsneal	Simple Share Buttons Adder	2.6	All	All	All

Application	Sharethis	Simple Share Buttons Adder	2.8	All	All	All
Application	Sharethis	Simple Share Buttons Adder	2.9	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.0	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.1	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.2	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.3	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.4	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.5	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.6	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.7	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.8	All	All	All
Application	Sharethis	Simple Share Buttons Adder	3.9	All	All	All
Application	Sharethis	Simple Share Buttons Adder	4.0	All	All	All
Application	Sharethis	Simple Share Buttons Adder	4.1	All	All	All
Application	Sharethis	Simple Share Buttons Adder	4.2	All	All	All
Application	Sharethis	Simple Share Buttons Adder	4.3	All	All	All
Application	Sharethis	Simple Share Buttons Adder	All	All	All	All

References

Reference	Source	Link
CSRF and stored XSS in Simple Share Buttons Adder 4.4 allows attackers to execute javascript – dxw advisories	MISC	security.dxw
WordPress › Simple Share Buttons Adder ‹ WordPress Plugins	CONFIRM	wordpress.c
Full Disclosure: CSRF and stored XSS in Simple Share Buttons Adder 4.4 (WordPress plugin)	FULLDISC	seclists.org
WordPress Simple Share Buttons Adder 4.4 CSRF / XSS ≈ Packet Storm	MISC	packetstorm
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 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](#).

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