



CVE-2014-4596

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

Summary

CVE	CVE-2014-4596
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-07-02 18:55:10 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple cross-site scripting (XSS) vulnerabilities in js/button-snapapp.php in the SnapApp plugin 1.5 and earlier for WordPr

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Snapapp Project	Snapapp	All	-	All	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	Link
WordPress SnapApp Plugin CVE-2014-4596 Multiple Cross Site Scripting Vulnerabilities			af854a3a-2127-422b-91ae-364da2661108	www.
wp-plugin : wpsnapapp – A3-Cross-Site Scripting (XSS) Code Vigilant			af854a3a-2127-422b-91ae-364da2661108	codev
CVE Program record			CVE.ORG	www.
NVD vulnerability detail			NVD	nvd.n
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				