



CVE-2014-5202

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

Summary

CVE	CVE-2014-5202
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-08-12 23:55:04 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Cross-site scripting (XSS) vulnerability in compfight-search.php in the Compfight plugin 1.4 for WordPress allows remote au

Risk And Classification

Primary CVSS: v2.0 3.5 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

Single

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Compfight Project	Compfight	1.4	-	-	All

Vendor Declared Affected Products				
Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified
References				
Reference	Source		Link	Tags
WordPress › Compfight « WordPress Plugins	af854a3a-2127-422b-91ae-364da2661108		wordpress.org	Package
WordPress Compfight 1.4 Cross Site Scripting ≈ Packet Storm	af854a3a-2127-422b-91ae-364da2661108		packetstormsecurity.com	Exploit
downloads.wordpress.org/plugin/compfight.1.5.zip	af854a3a-2127-422b-91ae-364da2661108		downloads.wordpress.org	Package
CVE Program record	CVE.ORG		www.cve.org	Canonical
NVD vulnerability detail	NVD		nvd.nist.gov	Canonical
No vendor comments have been submitted for this CVE.				
There are currently no legacy QID mappings associated with this CVE.				