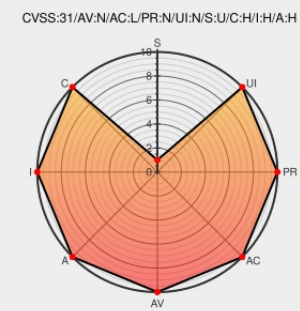
CVE-2015-9466

Published on: 10/10/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9466

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wti Like Post from Webtechideas contain the following vulnerability:

The wti-like-post plugin before 1.4.3 for WordPress has WtiLikePostProcessVote SQL injection via the HTTP_CLIENT_IP, HTTP_X_FORWARDED_FOR, HTTP_X_FORWARDED, HTTP_FORWARDED_FOR, or HTTP_FORWARDED variable.

CVE-2015-9466 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.5 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
WTI Like Post <= 1.4.2 - Unauthenticated Blind SQL Injection	Third Party Advisory, web.archive.org, text/html, Inactive Link, Not Archived	MISC wpvulndb.com/vulnerabilities/8318

WordPress › WTI Like Post « WordPress Plugins	Product Third Party Advisory wordpress.org text/html	MISC wordpress.org/plugins/wti-like-post/#developers
No Description Provided	Exploit Third Party Advisory cinu.pl text/html	MISC cinu.pl/research/wp-plugins/mail_576345187f5867ec8921b12de5884fb1.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Webtechideas	Wti Like Post	All	All	All	All
Application	Webtechideas	Wti Like Post	All	All	All	All

cpe:2.3:a:webtechideas:wti_like_post:*:*:*:*:*:wordpress:*:*:

cpe:2.3:a:webtechideas:wti_like_post:*:*:*:*:*:wordpress:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→