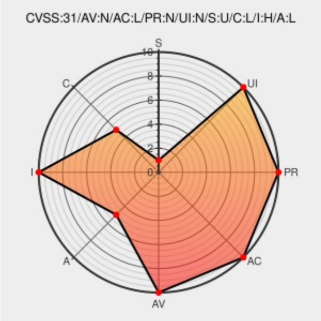
CVE-2021-36916

Published on: 11/24/2021 12:00:00 AM UTC

Last Modified on: 11/26/2021 03:49:00 PM UTC

CVE-2021-36916

Source: Mitre | Source: Nist | Print: PDF



Certain versions of Hide My Wp from Wpwave contain the following vulnerability:

The SQL injection vulnerability in the Hide My WP WordPress plugin (versions <= 6.2.3) is possible because of how the IP address is retrieved and used inside a SQL query. The function "hmwp_get_user_ip" tries to retrieve the IP address from multiple headers, including IP address headers that the user can spoof, such as "X-Forwarded-For." As a result, the malicious payload supplied in one of these IP address headers will be directly inserted into the SQL query, making SQL injection possible.

CVE-2021-36916 has been assigned by audit@patchstack.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **wpWave** - **Hide My WP (WordPress plugin)** version **<= 6.2.3**

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
Multiple Security Vulnerabilities Fixed In Hide My WP - Patchstack	patchstack.com text/html	MISC patchstack.com/hide-my-wp-vulnerabilities-fixed/
Hide My WP - Amazing Security Plugin for WordPress! by wpWave | CodeCanyon	codecanyon.net text/html	CONFIRM codecanyon.net/item/hide-my-wp-amazing-security-plugin-for-wordpress/4177158
WordPress Hide My WP premium plugin <= 6.2.3 - Unauthenticated SQL injection (SQLi) vulnerability - Patchstack	patchstack.com text/html	MISC patchstack.com/database/vulnerability/hide-my-wp/wordpress-hide-my-wp-premium-plugin-6-2-3-sql-injection-sqli-vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wpwave	Hide My Wp	All	All	All	All

cpe:2.3:a:wpwave:hide_my_wp:*:*:*:*:wordpress:*:*:

Discovery Credit

Vulnerability discovered by Dave Jong (Patchstack).

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-36916 : The SQL injection vulnerability in the Hide My WP WordPress plugin versions <= 6.2.3 is possible… twitter.com/i/web/status/1…	2021-11-24 17:05:48

← Previous ID

Next ID→

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 registred 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