Me Broccoli

TS Poll <= 2.4.6 - Authenticated SQL Injection (CVE-2025-3470)

Parikesit

April 14, 2025

0

Olá Broccolitos.. I discovered an Authenticated SQL Injection vulnerability in the WordPress plugin TS Poll – Survey, Versus Poll, Image Poll, Video Poll version <= 2.4.6. This vulnerability has been assigned CVE-2025-3470 and is now publicly listed in the Wordfence Intelligence Vulnerability Database.

Vulnerability Details

The vulnerability resides in the s POST parameter in the following endpoint:

> /wp-admin/admin.php?page=ts-poll

Due to insufficient input sanitization, an authenticated attacker (Administrator+) can inject arbitrary SQL commands into the query, allowing unauthorized access to database contents.

Me Broccoli

Proof of Concept:

1. Install the plugin and log in as an administrator.
2. Go to: wp-admin/admin.php?page=ts-poll
3. In the search bar, enter any query and intercept the request using Burp Suite.
4. Save the intercepted request to a file.
5. Run the following sqlmap command:

```
sqlmap -r [requestfile] -p s --random-agent --
tamper=space2comment --level 5 --risk 3
```

The parameter s is confirmed to be vulnerable.

Plugin developers have patched this issue in version 2.4.7. It is strongly recommended to update to the latest version immediately.

Reference:
Changeset Source Code

Database Vulnerability

Thats all from me,
Hasta Luego Broccolitos!!!

0 Comments