Vulnerability Advisory

ISEC-V2021-03

FV Flowplayer Video Player WordPress plugin
Reflected XSS on administrator dashboard page

INTRINSEC

Innovative by design

TOUR CBX, 20ème ETAGE, 1 PASSERELLE DES REFLETS, 92913 PARIS LA DEFENSE CEDEX • TEL +33 1 41 91 77 77
INTRINSEC SECURITE • SAS AU CAPITAL DE 2 760 680 € • SIREN : 812 535 284 • APE : 6203Z

ADVISORY ISEC-V2021-03

Vendor: FolioVisio

Product: FV Flowplayer Video Player

Title: Reflected XSS on administrator dashboard page

Intrinsec ID: ISEC-V2021-03

Published: 15/10/2021

Last updated: 19/07/2021

Risk: Moderate

Exploitation: remote

Impact:

- Security feature bypass
- Sensitive data exposure
- Application's users compromise
- Privilege escalation

Description: An input query string is reflected on the dashboard without being checked. As a result, it is possible through this input to execute arbitrary JavaScript code in the browser where the request is sent. An attacker could therefore generate a malicious link and send it to application administrators. The attacker would then be able to send requests on behalf the compromised administrator and, for instance, create a new administrator account in order to gain persistence on the application. This could also lead to phishing or keylogging, which could for example lead to the interception of credentials in order to gain access to a session and impersonate a user.

Vulnerable versions: 7.5.0.727 to 7.5.3.727 excluded

Solutions: Check the user input using one of the following methods:

- Checking that it is an integer;
- Encoding data before displaying.

Credits: Vulnerability discovered by Margaux DABERT from Intrinsec.

History:

2021-07-19: Vulnerability identified

2021-08-12: Communication with the plugin editor

2021-09-07: Communication of the advisory to WordPress

2021-10-05: Obtaining the CVE number CVE-2021-39350

DETAILED APPROACH

While reviewing the source code of the FV Flowplayer Video Player plugin, we identified in the */view/stats.php* file that a URL parameter was reflected on the administrator dashboard without being filtered.

```
// view/stats.php : Lines 5-7 and 191-195
if( isset($_GET['player_id']) && intval($_GET['player_id'])  ) {
    $fv_single_player_stats_data = $FV_Player_Stats-
>get_player_stats( intval($_GET['player_id']) );
}

[…]

<?php elseif ( isset($fv_single_player_stats_data) ): ?>
  <div>
    <h2>No Plays For Player <?php echo $_GET['player_id']; ?> in past week</h2>
  </div>
<?php endif; ?>
```

In this code snippet, the GET “player_id” parameter is used without checking its format. An attacker could then inject JavaScript code through this parameter. The browser will then execute the code when the page is loaded if the following conditions are met:

- The parameter “player_id” exists;
- The value of the “player_id” parameter is a string which is numeric or which can be converted to a numerical value (for example, when it starts with a number no matter what characters follow).

Therefore, as soon as the parameter takes the value of a string beginning with a number, the first condition is verified. The variable “fv_single_player_stats_data” is then defined, which allows to validate the second condition above. With this second condition, the GET parameter “player_id” is displayed on the page. An attacker can introduce arbitrary JavaScript code by taking care to start the string with a numeric value. This leads to a reflected XSS attack.

An attacker could use this flaw in a phishing campaign for example to:

- Create an administrator access or any other adminsitrator action;
- Steal session cookies and thus authenticate as a user (in case the HttpOnly attribute is not set);
- Attempt to steal a user's credentials using social engineering methods (fake authentication pop-up for example);
- Redirect the user to a malicious site.