

New issue

[Jump to bottom](#)

## Remote Code Execution (RCE) in SoyCMS #9

🔒 Closed stypr opened this issue on Sep 14, 2020 · 0 comments · Fixed by #14

stypr commented on Sep 14, 2020

Contributor

### Title

Remote Code Execution (RCE) in SoyCMS

### Summary

Severity: High

SoyCMS 3.0.2 and earlier is affected by Remote Code Execution (RCE) using Unrestricted File Upload. Cross-Site Scripting(XSS) vulnerability that was reported earlier can be chained in order to perform a successful remote code execution by redirecting the administrator to load a specially crafted webpage.

Impact: XSS to RCE via Inquiry Error and Unrestricted File Upload

- Attack vector is: Administrator must be logged in.
- Components are: File Manager
- Tested SoyCMS Version : 3.0.2 (latest)
- Affected SoyCMS Version : ~3.0.2

Found by @stypr from Vulnerability Research Team in [Flatt Security Inc.](#)

Full Exploit Video: <https://youtu.be/FWIDFNXmr9g>

### Cause

The file upload feature in FileManager is using elFinder. However, it was found out that mimetype can be fooled to upload a PHP file. There is no feature in elFinder to check the file type so it needs to be manually implemented.

[soycms/cms/soycms/js/elfinder/php/connector.php](#)  
Lines 143 to 159 in 34e066d

```
143     $opts = array(  
144         // 'debug' => true,  
145         'roots' => array(  
146             // Items volume  
147             array(  
148                 'driver'     => 'LocalFileSystem',      // driver for accessing file system (REQUIRED)  
149                 'path'       => $path,                // path to files (REQUIRED)  
150                 'URL'        => $url,                // URL to files (REQUIRED)  
151                 // 'treeDeep' => 1,                  // elFinder's back of tree folder
```

[soycms/cms/soycms/js/elfinder/php/connector.php-change2](#)  
Lines 188 to 215 in 4375940

```
188     array(  
  
189         'driver'     => 'LocalFileSystem',  
  
190         'path'       => $path,  
  
191         // 'startPath' => $site->getPath(),  
  
192         'URL'        => $url,  
  
193         // 'treeDeep' => 3,
```

### Remediation

Please add a file extension check from accessControl.

<https://github.com/Studio-42/elFinder/blob/b3e92120a8657bdd263ad750dc9760c8d5aa2a89/php/connector.minimal.php-dist#L47-L59>

🔗 This was referenced on Sep 15, 2020



**Fix Cross-Site Scripting: Print error message instead #13**

➔ Merged

**Fix RCE: Block PHP extension upload #14**

➔ Merged

 inunosinsi closed this as completed in #14 on Sep 16, 2020

  **styprr** mentioned this issue on Sep 16, 2020

**Request for creating a Security Advisory #17**

 Closed

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

Successfully merging a pull request may close this issue.

 [Fix RCE: Block PHP extension upload](#)

1 participant

