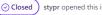


<> Code ○ Issues \$\mathcal{1}\$ Pull requests ○ Actions □ Projects ① Security 4 \(\subseteq \) Insights

Jump to bottom New issue

Unauthenticated Remote Code Execution (RCE) in SoyCMS #10



stypr commented on Sep 14, 2020

⊙ Closed stypr opened this issue on Sep 14, 2020 · 1 comment · Fixed by #12

Title

Unauthenticated Remote Code Execution (RCE) in SoyCMS

Summary

Severity: Critical

SoyCMS 3.0.2 and earlier is affected by Unauthenticated Remote Code Execution (RCE). The allows remote attackers to execute any arbitrary code when the inquiry form feature is enabled by the website. The vulnerability is caused by unserializing the form without any restrictions.

Impact: Unauthenticated Remote Code Execution via Inquiry Form

- Attack vector is: Inquiry Form needs to be enabled.
- Components are: Soy Inquiry Form
- 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/zAE4Swjc-GU

When the inquiry is submitted and the captcha is taken, form submits form_value and form_hash, and value is checked as the following.

```
soycms/cms/app/webapp/inquiry/page.php
Lines 126 to 133 in 0373eb1
126
         if(isset($_POST["form_value"]) && isset($_POST["form_hash"])){
127
                $value = base64_decode($_POST["form_value"]);
129
                //不正な書き換えでない場合のみ
130
                if(md5($value) == $_POST["form_hash"]){
131
                         $_POST["data"] = unserialize($value);
132
                }
133
```

By the PHP's official guideline, unserialize is a function that should not be used when user can control the argument (Reference: https://www.php.net/manual/en/function.unserialize.php)

md5(\$value) == form_hash can be generated locally, so it is possible to control this value and use appropriate classes to trigger code execution.

Remediation

Use json_encode and json_decode instead.

I will make a Fix PR as soon as possible.

stypr mentioned this issue on Sep 14, 2020

Change serialize/unserialize to json encode/decode #11

(1 Closed)

stypr commented on Sep 14, 2020

Contributor Author

Contributor

The previous PR had a collision with DAO column verification. I will check and make a proper fix.

stypr mentioned this issue on Sep 15, 2020

Fix RCE: Change serialize/unserialize to json encode/decode #12

(♣ Merged)

inunosinsi closed this as completed in #12 on Sep 16, 2020

stypr mentioned this issue on Sep 16, 2020

Request for creating a Security Advisory #17

⊙ Closed

No one assigned
Labels
None yet
Projects
None yet
Milestone
No milestone
Development
Successfully merging a pull request may close this issue.
s Fix RCE: Change serialize/unserialize to json encode/decode

1 participant

