# Stored XSS Vulnerability in Chronoforum v2.0.11 (Joomla plugin)

Jump to bottom

nugmubs edited this page on Nov 16, 2020  $\cdot$  6 revisions

# **Vulnerability Information**

- Vendor: Chronoforums v2.0.11 (Joomla's plugin)
- Vulnerability : Stored XSS
- Impact : Joomla Homepage with the chronoforum plug-in

A Stored XSS vulnerability was found in the installable Chronoforums extension plug-in on Joomla's Plug-in Install page.

# Discoverer

• nugmubs in Naver Business Platform (NBP)

#### Product

- chronoforums v2.0.11
- Chronoforums\_v2.0.11\_Extension.zip

# **Update Version**

• It's still vulnerable.

# History

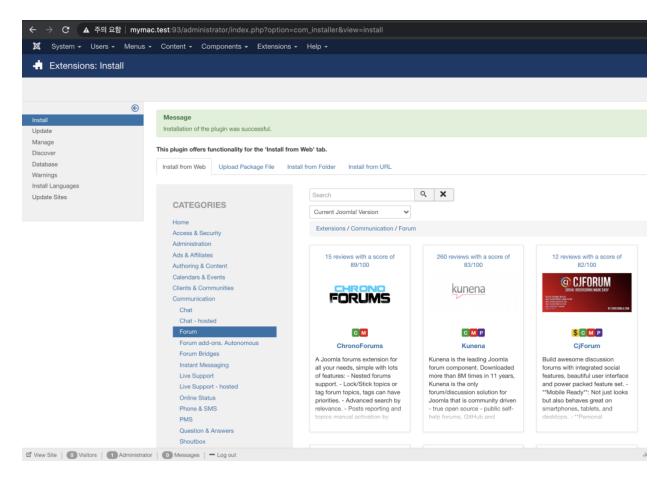
- 2020.08.26 Inform the vulnerability to chronoengines.com
- 2020.11.16 It still has the vulnerability

# Overview of Vulnerability

ChronoForms 2.0.11 is affected by: Stored Cross Site Scripting (Stored XSS). The impact is: execute JavaScript in victim's browser, when the vulnerable page is loaded.

# 1. Install Chronoforum in Joomla plugin Installation Page.

• Install Chronoforum in Joomla Admin Page



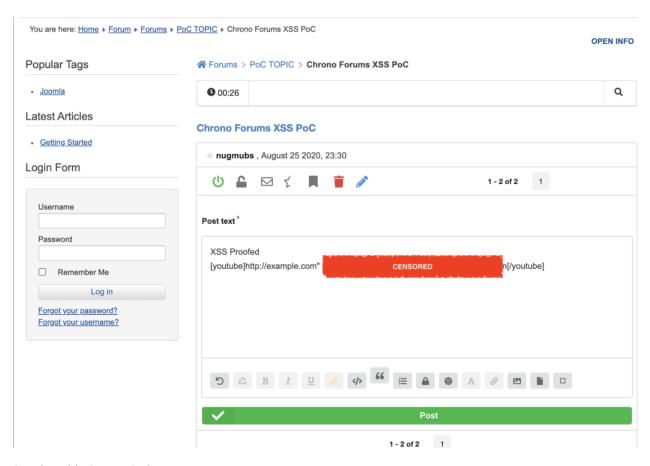
# 2. Inject Payload

The vulnerability exists when you enter Payload below in the New Topic creation screen of the Forum.

The JavaScript (semantic.min.js) creates an iframe, which results in the saved Payload operation resulting in an XSS vulnerability.

An attacker can steal a user's cookies or engage in malicious behavior through a stored XSS.

Vulnerable Payload: [youtube]http://example.com" onload="alert('XSS Proofed')" http://example.com[/youtube]



# 3. Vulnerable Source Code

com\_chronoforums2 extension accepts unsanitized inputs and stores it in the database. please, see the below picture.

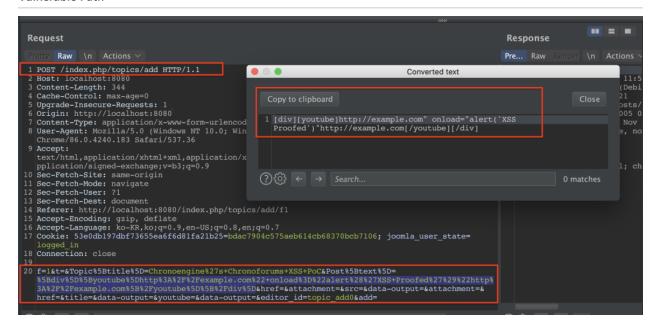
When the payload([youtube]http://example.com" onload="alert('XSS Proofed')" http://example.com[/youtube]) is rendered on any browsers(Chrome, Safari, Firefox), injected payload is evaluated, then execute malicious javascript code.

 $/components/com\_chronoforums2/chronoforums/controllers/topics.php:381$ 

If an unsanitized source object contained an enumerable proto property, it could extend the native Object.prototype.

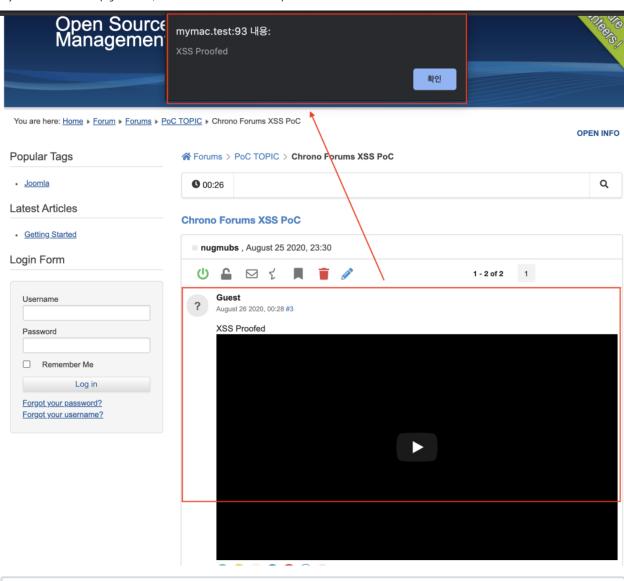
```
works — docker exec -it joomla-latest_joomla_1 /bin/bash — 136×52
                                                  return ['error' => rl('You have to wait some time before you can make a new post.'),
       => true];
359
                                                  \GApp::session()->set('last_forum_post', time());
363
364
365
366
367
368
                                $postsController = $this->getController('posts');
                                $topic = [];
$topic['title'] = $this->data['Topic']['title'];
$topic['published'] = (int)($this->get('settings.auto_publish_topics', 00 OR \GApp::access('chronoforums',
    topics moderate'));
369
370
371
372
373
374
375
376
377
378
389
381
382
383
384
385
                                $topic['forum_id'] = $this->data['f'];
                               $topic['published'] = (int)$auto_approval;
                                $result = $this->Topic->store($topic, $this->data('Post.text'), $this->data('Attachment', []));
if($result !== true){
                                         return array_merge($result, ['reload' => true]);
                                //save tags
if((int)$this->get('settings.enable_topics_tags', 1) AND !empty($this->data['tags']) AND count($this
```

#### **Vulnerable Path**



#### 5. PoC

Payload When the inserted page is loaded, the inserted code acts and the script runs.



Find a page...

Home

Stored XSS Vulnerability in Chronoforum v2.0.11 (Joomla plugin)

Vulnerability Information
Discoverer
Product
Update Version
History
Overview of Vulnerability

1. Install Chronoforum in Joomla plugin Installation Page.
2. Inject Payload
3. Vulnerable Source Code
Vulnerable Path
5. PoC

# Clone this wiki locally

https://github.com/nugmubs/chronoforums-cve.wiki.git

L C