0-DAY NO CVE HIGH PUBLIC

OpenCart reward + Free Checkout, authenticated underpay

OpenCart 4.1.0.4 reward.save unsets session.reward and never payment_method. coupon.save does. Apply points, pick Free Checkout, clear points, confirm writes catalog total, free_checkout.confirm does not recheck. No CVE yet.

NAME OpenCart reward + Free Checkout, authenticated underpay	TYPE 0-day analysis
CVE n/a	CVE RISK high
DISCLOSURE STATUS public	VENDOR OpenCart
AFFECTED OpenCart through 4.1.0.4 reward + Free Checkout; unpublished. Distinct from coupon race CVE-2025-15116. Guest checkout is not this bug.	PUBLISHED 26 Sept 2026
UPDATED 26 Sept 2026	TAGS 0-day, opencart, free-checkout, reward, cwe-840, cwe-863, authenticated

TL;DR

Lab files and proof-of-concept **here**.

01 coupon.save learned. reward.save did not

I am @abraxas_null. The proof of concept is on GitHub: **abraxas/opencart-reward-free-checkout** (loopback client). The lab stack is `lab/`: Dockerfile, docker-compose.yml, run.sh, setup-opencart.sh. Authorized lab only. It talks to loopback.

This is **OpenCart 4.1.0.4**, reward points plus Free Checkout. No CVE yet. CWE-840 / CWE-863. 6.5 High (`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N`). Logged-in customer with points. Not a shell. Not unauthenticated. Guest cart is not this bug.

CVE-2025-15116 was a coupon race through 4.1.0.3. On 4.1.0.4, `coupon.save` unsets `payment_method` when the coupon changes. `reward.save` does not. Apply enough points that `getTotals` is `≤ 0.00`, pick Free Checkout, then clear the points. `confirm` `editOrder`s the pending row to catalog price. `free_checkout.confirm` only checks the session payment code. Lab order **4**: `total=100.00`, `order_status_id=1`, Free Checkout, points balance still **1000**. No debit.

I am not printing a checkout POST sequence you can paste at someone else's `/index.php?route=`. The missing `unset($this->session->data['payment_method'])` is the useful part. Isolated lab. The stack is in the GitHub repo so you can run it at home.

02 What an attacker can do

Log in, put a points-covered SKU in the cart, apply enough reward that Free Checkout lists, save that method, then `reward.save` with `0`. Second confirm writes catalog total. `free_checkout.confirm` promotes the order to paid. Points never debit.

They do not get a shell. Guest checkout is not this bug: reward needs a customer. Free Checkout only *lists* at `total ⩽ 0`. The bug is that clearing points does not unlist it, and confirm does not look at the total again.

03 The lab (run this at home)

Source of truth is `lab/`. Image `php:8.2-apache`. Compose also runs `mysql:8.0`. Port **18108**. Bind it to loopback. Place OpenCart **4.1.0.4** `upload/` at `lab/www`. That tree is not in the GitHub repo.

DOCKERFILE Copy

```
FROM php:8.2-apache

RUN apt-get update \
  && apt-get install -y --no-install-recommends wait-for-it unzip libfreetype6-d
  && docker-php-ext-configure gd --with-freetype --with-jpeg --with-webp \
  && docker-php-ext-install -j$(nproc) gd zip mysqli curl \
  && docker-php-ext-enable gd zip mysqli curl \
  && a2enmod rewrite \
  && rm -rf /var/lib/apt/lists/*

WORKDIR /var/www/html
```

`docker-compose.yml`:

YAML Copy

```
name: opencart-reward-free-checkout

services:
  mysql:
    image: mysql:8.0
    command: --default-authentication-plugin=mysql_native_password
    environment:
      MYSQL_ROOT_PASSWORD: opencart
      MYSQL_DATABASE: opencart
    healthcheck:
```

```
      test: ["CMD", "mysqladmin", "ping", "-h", "127.0.0.1", "-uroot", "-popenca
      interval: 5s
      timeout: 5s
      retries: 40
      start_period: 20s

  opencart:
    build: .
    ports:
      - "127.0.0.1:18108:80"
    volumes:
      - ./www:/var/www/html
      - ./setup-opencart.sh:/startup/setup-opencart.sh:ro
    command: >
      bash -c "wait-for-it mysql:3306 -t 90 && bash /startup/setup-opencart.sh &
    depends_on:
      mysql:
        condition: service_healthy
    environment:
      PHP_MEMORY_LIMIT: 512M
```

`setup-opencart.sh` runs `install/cli_install.php`, then the fixture. Demo product **36** (iPod Nano) already has `points=100`. The seed drops tax and shipping so reward can zero `getTotals` exactly. That is not the bug. A catalog SKU whose points cover the line is the realistic case. Customer `oc-reward@localhost.invalid` gets **1000** points.

PHP Copy

```php
$m->query("UPDATE oc_product SET shipping=0, tax_class_id=0, points=100, status=1
// INSERT oc_customer oc-reward@localhost.invalid
$m->query("INSERT INTO oc_customer_reward (customer_id,order_id,description,point
```

`total_reward_status=1` and `payment_free_checkout_status=1` are defaults.

PLAIN TEXT Copy

```
git clone https://github.com/abraxas/opencart-reward-free-checkout
# put opencart 4.1.0.4 upload/ at lab/www

```

```
cd opencart-reward-free-checkout/lab
./run.sh
```

`run.sh` builds, waits for catalog HTTP 200, then runs the client. The proof of concept is written for `127.0.0.1:18108`. Do not publish the port off loopback.

04 What the tree actually unsets

`Reward::save` on 4.1.0.4:

PHP Copy

```php
if (!$json) {
    $json['success'] = $this->language->get('text_success');

    if ($reward) {
        $this->session->data['reward'] = $reward;
    } else {
        unset($this->session->data['reward']);
    }
}
```

That is the whole mutation. `reward=0` drops `session.reward`. It does not touch `payment_method`. Compare `Coupon::save` after the coupon is accepted:

PHP Copy

```php
$this->session->data['coupon'] = $coupon;

unset($this->session->data['payment_method']);
unset($this->session->data['payment_methods']);
```

`FreeCheckout::getMethods` is honest about when the method exists:

PHP Copy

```
($this->model_checkout_cart->getTotals)($totals, $taxes, $total);

$status = ($total <= 0.00) && !$this->cart->hasSubscription();
```

List it while points zero the cart. Save `free_checkout.free_checkout`. First `checkout/confirm.confirm` `addOrder`s a pending row (`order_status_id=0`) at total **0**. Then `reward.save` with `0` clears the points and leaves the payment code. Second confirm:

PHP Copy

```
if (!$order_id) {
    $this->session->data['order_id'] = $this->model_checkout_order->addOrder($orc
} elseif ($order_info && !$order_info['order_status_id']) {
    $this->model_checkout_order->editOrder($order_id, $order_data);
}
```

Pending orders are rewritten. Catalog total. Same `payment_method`. Then `FreeCheckout::confirm`:

PHP Copy

```
if (!isset($this->session->data['payment_method']) || $this->session->data['payme
    $json['error'] = $this->language->get('error_payment_method');
}

if (!$json) {
    $this->model_checkout_order->addHistory($this->session->data['order_id'], $th
    $json['redirect'] = $this->url->link('checkout/success', 'language=' . $this-
}
```

Session code only. No `total <= 0.00`. No re-run of `getMethods`. No point debit. `addHistory` promotes status **0** to **1**. The customer still has the 1000.

HTTP is `POST /index.php?route=extension/opencart/checkout/reward.save`. Function names in the write-up are PHP methods. OpenCart 4 routes are

`controller.method`.

05 The 200 that paid with points

The first client that looks at this will apply 100 points, pick Free Checkout, confirm once, and get an honest zero-total order. That is not the bug. That is the feature.

A few other ways to lose without learning anything:

- `coupon.save` instead of `reward.save`. That path unsets the method. CVE-2025-15116 leftover.
- Guest checkout. Reward needs a customer.
- Product with `points=0`. Free Checkout never lists.
- Leaving `reward` in session through `free_checkout.confirm`. Honest free order, points should debit.
- Looking at `order_status_id=0` only. Pending is not paid. The oracle is **status 1, total 100.00, payment free_checkout, debit 0**.
- A reverse shell. Theatre. The witness is the order row.

Lab catalog **100.00**. iPod Nano `product_id=36`. After the clear: order **4** `total=100.0000` `status=0` still `free_checkout.free_checkout`. Then `free_checkout.confirm` redirects `checkout/success`. Final: `status=1` `debit=0` `balance=1000`.

06 What I actually did

Treat the on-disk product as the spec. I read `reward.save`, then `coupon.save`, then `getMethods` (`total ⩽ 0.00`), then `editOrder` while status is 0, then `free_checkout.confirm`. Proof of concept: opencart-reward-free-checkout-Abraxas-Labs.py.

Login, cart, stamp Free Checkout, clear points, confirm, lookup. Customer login. Cart add 36. `reward.save` 100. Payment methods list Free Checkout. Save it. Confirm writes order 3 at 0. `reward.save` 0. Confirm rewrites order 4 at 100.00. `free_checkout.confirm`. I am not reprinting `OCSESSID`.

Last lab run, trimmed:

PLAIN TEXT Copy

```
SUCCESS OpenCart reward + Free Checkout underpay
IOC order-after-reward 3 total=0.0000 status=0 free_checkout.free_checkout
IOC order-after-clear 4 total=100.0000 status=0 free_checkout.free_checkout
IOC free_checkout.confirm redirect checkout/success
IOC order-final 4 total=100.0000 status=1 debit=0 balance=1000
```

The client that produced it is on GitHub.

Wrong turns already recorded: `coupon.save` instead of `reward.save` (that path unsets the method); guest checkout; product with `points=0` (Free Checkout never lists); leaving `reward` in session through `free_checkout.confirm` (honest free order, points should debit); looking at `order_status_id=0` only (pending is not paid). The oracle is **status 1, total 100.00, payment free_checkout, debit 0**.

07 What this is not

It is not CVE-2025-15116. That was a coupon race. This is sequential, authenticated, and on the reward controller the coupon hardening missed. It is not "Free Checkout always ships catalog SKUs." The method only *lists* at `total ⩽ 0`. The bug is that

clearing points does not unlist it, and confirm does not look at the total again. It is not unauthenticated. It is not RCE.

08 The fix

`unset` `payment_method` in `reward.save` the way `coupon.save` already does, and make `free_checkout.confirm` refuse `total > 0`. Re-run the loopback client against a patched build: `oc_order.total` must not sit at catalog price with Free Checkout and no point debit.

I am not going to print a storefront POST you can paste at someone else's checkout. The missing unset is the useful part. If you own the box, run the proof of concept against loopback.

09 References

- Proof of concept: abraxas/opencart-reward-free-checkout · opencart-reward-free-checkout-Abraxas-Labs.py
- Lab: `lab/` · Dockerfile · docker-compose.yml · run.sh · setup-opencart.sh
- @abraxas_null · github.com/abraxas · abraxaslabs.tech · abraxas.null@proton.me
- CWE-840 · CWE-863
- 4.1.0.4: `reward.php` · `coupon.php` · `free_checkout.php` controller · `free_checkout.php` model · `confirm.php`
- Contrast: CVE-2025-15116 (NVD)

- tag 4.1.0.4 · README security
- Product: OpenCart · opencart.com

Abraxas Labs

Independent security research by abraxas.

Analysis of 0-days, n-days, malware, and the

leftovers that still matter.

GitHub **@abraxas_null** **abraxas.null@proton.me** **abraxaslabs.tech**

Independent research. Private analysis by arrangement. No ads. abraxas.null@proton.me · For defensive awareness and authorized testing only.

© 2026 Abraxas Labs