Unauthenticated Access to Payment Order Data via BlockonomicsYPT check.php

Low **DanielnetoDotCom** published **GHSA-3v7m-qg4x-58h9** 4 days ago

Software

WWBN/AVideo

Affected versions

<= 26.0

Patched versions

None

Description

Severity: Low
CWE: CWE-862 (Missing Authorization)

Summary

The BlockonomicsYPT plugin's `check.php` endpoint returns payment order data for any Bitcoin address without requiring authentication. The endpoint was designed as an AJAX polling helper for the authenticated `invoice.php` page, but it performs no access control checks of its own. Since Bitcoin addresses are publicly visible on the blockchain, an attacker can query payment records for any address used on the platform.

Details

In `plugin/BlockonomicsYPT/check.php` at lines 20-30, the endpoint accepts a Bitcoin address and returns the corresponding order data:

```
$addr = $_GET['addr'];
$order = new BlockonomicsOrder(0);
$obj = $order->getFromAddressFromDb($addr);
die(json_encode($obj));
```

There is no authentication check. The endpoint does not verify that the requesting user is logged in, nor does it verify that the requesting user owns the order associated with the given address.

The response includes:

- User ID of the buyer
- Total payment value
- Currency
- BTC amounts (expected and received)
- Transaction ID
- Payment status

The `invoice.php` page that was designed to consume this endpoint does require authentication, but `check.php` itself does not inherit or enforce that requirement.

Bitcoin addresses are publicly queryable on the blockchain, so an attacker does not need to guess them. Addresses associated with the platform can be discovered by monitoring blockchain transactions to known platform wallets.

The BlockonomicsYPT plugin is tagged as deprecated by the AVideo project, but remains available and functional in current installations.

Proof of Concept

```
# Query payment data for a known Bitcoin address without authentication
curl "https://your-avideo-instance.com/plugin/BlockonomicsYPT/check.php?addr=1A1zP
```

Example response:

```
{
  "id": 42,
  "users_id": 15,
  "value": "29.99",
  "currency": "USD",
  "btc_value": "0.00085",
  "btc_received": "0.00085",
  "txid": "abc123def456...",
  "status": "confirmed",
  "created": "2025-01-15 10:30:00"
}
```

No session cookie or API key is required.

Impact

- Unauthenticated disclosure of payment order data including user IDs, amounts, and transaction details
- Bitcoin addresses are publicly discoverable on the blockchain
- Links on-chain transactions to specific platform user IDs
- Privacy violation for users who made cryptocurrency payments on the platform
- Plugin is deprecated but still functional in existing deployments

Recommended Fix

Add an authentication check at `plugin/BlockonomicsYPT/check.php:17`:

```php
if (!User::isLogged()) {
    echo json_encode(["error" => "Login required"]);
    exit;
}
```

Found by aisafe.io

Severity

Low 3.7 / 10

CVSS v3 base metrics

Attack vector	Network
Attack complexity	High
Privileges required	None
User interaction	None
Scope	Unchanged
Confidentiality	Low
Integrity	None
Availability	None

Learn more about base metrics

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE ID

CVE-2026-35448

Weaknesses

▶ CWE-862

Credits

 **adrgs** Reporter

 **aisafe-bot** Finder