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	Patched versions
<= 6.5.2	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.

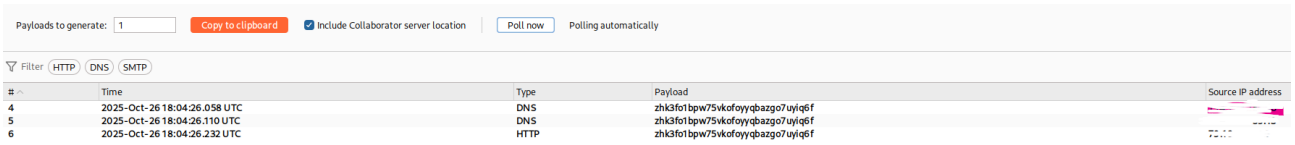
Details

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
```



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