rConfig Vulnerability Report

Daniel Elkabes, WhiteSource Software

Abstract

In this report we'll show a potential path traversal vulnerability in rConfig, this vulnerability still exists in the latest version 3.9.3.

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N | **7.5 (High)**

Issue Identified

As part of our routine analysis in WhitSource Software we found out that in downloadFile.php, there is a mishandeling with sanitizing the path variable.

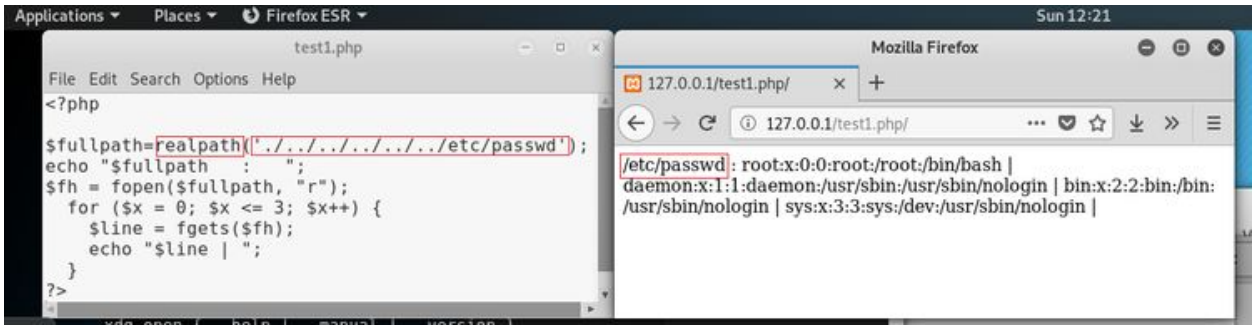
Firstly let's examine this section of code:

```
// realpath used to prevent path traversal exploit
$fullPath = realpath($_GET['download_file']);
```

We can see that the only sanitization done to the variable is by using "realpath".

Realpath function wasn't dedicated to do sanitization to paths, It simply converts a path and expands "../" into the right folder.

Let's see an example of a path traversal that could happen:



In the above example we can see a case where the path argument is build from multiple "../", which in this case means we'll succeed to get to the root folder no matter where we currently are (we can extend the number of "../" how much we want).

Then we can see another check in the code:

```
foreach ($pathWhiteList as $WhitePath) {
    if (0 === strpos($fullPath, $WhitePath)) {
```

This will use strpos function to check if one of the “$pathWhiteList” array values exist, and this isn’t sufficient check either.

We can see in the example below that we are checking if “$findme” exist in “$mystring”

```
$mystring = 'abc';
$findme   = 'a';
$pos = strpos($mystring, $findme);
```

This means that in rConfig code we are checking if one of the “whitepath” values exist in the “fullpath”, instead of comparing it to the beginning of the path.

Which means that the path shown below for example will pass the check:

“/classified/home/rconfig/logs/company/client/logs”

Although the scope of the path traversal is limited, it still exists and need to be handled.