TARTU ÜLIKOOOL
Loodus- ja täppisteaduste valdkond
Arvutiteaduse instituut
Informaatika õppekava

CVE-2017-14722

Kerttu Talts

Tartu 2018
INTRODUCTION

WordPress is the most popular website management system in use on the web. It was released on 27th of May 2003 by Matt Mullenweg and Mike Little. WordPress users can choose from different themes or create ones themselves to alter the look of their web page by not altering the core code or site content. The security vulnerability is directly connected to the user choosing the themes in WordPress. [5]

Security vulnerability CVE-2017-14722 is a vulnerability in WordPress earlier versions of 4.8.2. Priority of the security hole is stated “Medium”, because it’s possible to perform a Directory Traversal (aka dot-dot-slash) attack via a crafted theme filename. [1]

DESCRIPTION OF THE SECURITY VULNERABILITY

Because of the vulnerability, it’s possible to attack path traversal attack. Where the user can send a specially crafted theme filename to take advantage of the path traversal flaw [2]. It basically means that the user can attack the system by changing the themes filename to something like “.././.././../directory/filename”. This way the user can access files in server that should be accessible to only server administrators. For example in this way it’s possible to access some password files or some other sensitive information. The repetitive ../ is used to traverse (backtrack) directories in the server. [3] It is also possible for the attacker to attack by sending the end-user to an URL outside of this server by simply doing something similar:

http://some_site.com/some-page?page=page_that_attacker_wanted_to_send_the_user.html

The concept of this is also page traversal, through this it’s possible to include files and scripts located on external websites. [3, 4]

The vulnerability is caused by improperly validating user supplied input by the Customizer component.

REMEDY / FIX

As an end-user it is possible to fix the vulnerability by just upgrading to the latest version of WordPress (4.8.2 or later).

In the code the WordPress developers added a check to check if the theme filename is valid or not to remove the path traversal flaw.
In the following picture we can see that there is an additional check to see if the filename is valid [6]

The red line is the code before and green line is the fixed code. As we can see in the code before there were no additional checks for the filename.

The added function call `validate_file()` checks if the argument is valid. The method returns 0 if its valid path and 1 if its an invalid path. [7].

For example [7]:

**Valid file path**

```bash
$path = 'uploads/2012/12/my_image.jpg';
return validate_file( $path ); // Returns 0 (valid path).
```

**Invalid file path**

```bash
$path = '..../wp-content/uploads/2012/12/my_image.jpg';
return validate_file( $path ); // Returns 1 (invalid path).
```

So this means that the possibility to do a Directory Traversal attack is removed and the flaw is fixed.
REFERENCES

2. https://www.securitytracker.com/id/1039553
3. https://www.owasp.org/index.php/Path_Traversal
6. https://core.trac.wordpress.org/changeset/41397