

New issue



v3.8.0存在zip Bomb漏洞 #8199

Closed



lem0n817 opened 2 weeks ago



版本号：

v3.8.0

问题描述：

1. 概述

JeecgBoot的上传文档库功能存在zip 炸弹漏洞。

- 漏洞路径
后台-->AI大模型-->AI知识库-->文档库上传

2. 漏洞影响

- 系统资源（磁盘空间）被大量占用，导致服务不可用。

3. 漏洞成因

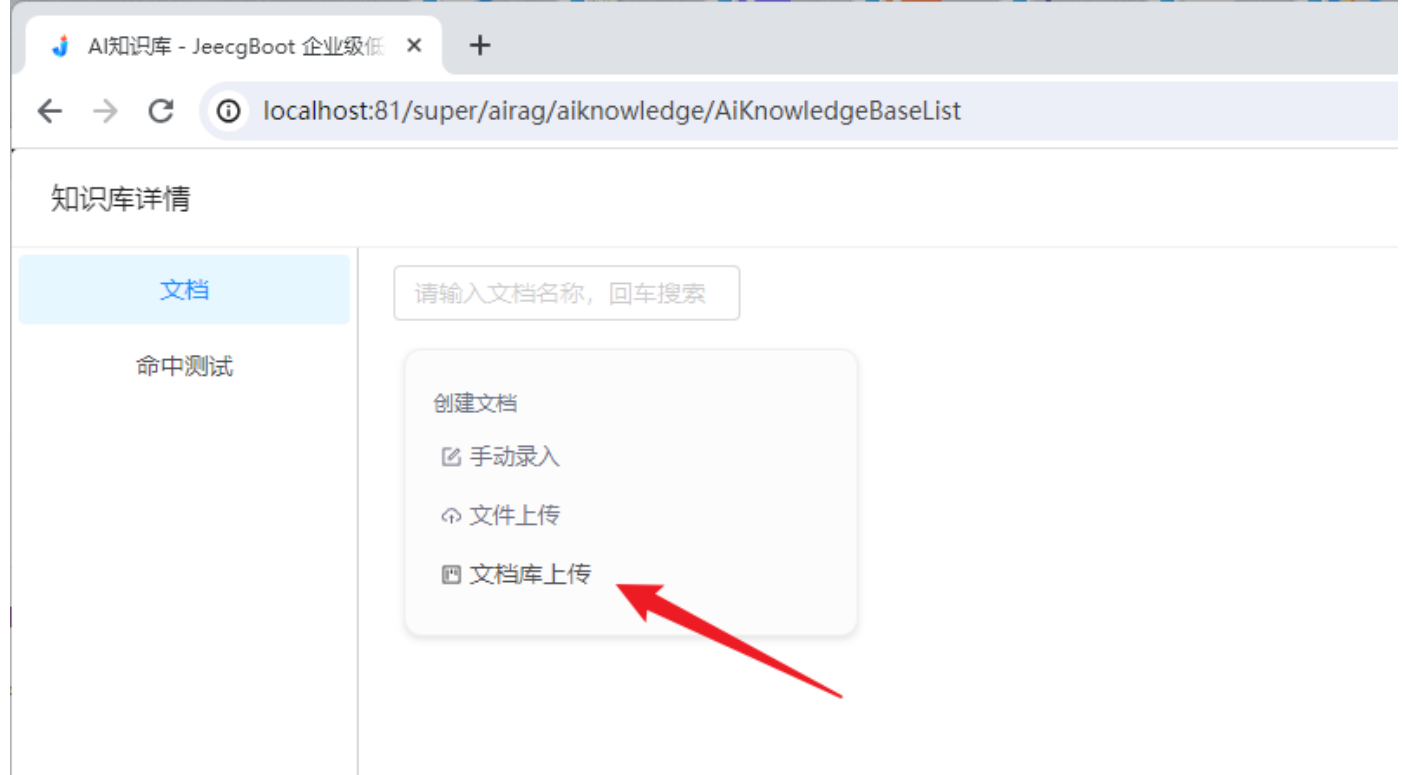
org.jeecg.modules.airag.llm.service.impl.AiragKnowledgeDocServiceImpl#unzipFile

仅对ZIP路径穿越做限制，并未对解压后文件的总大小和文件数量做限制。

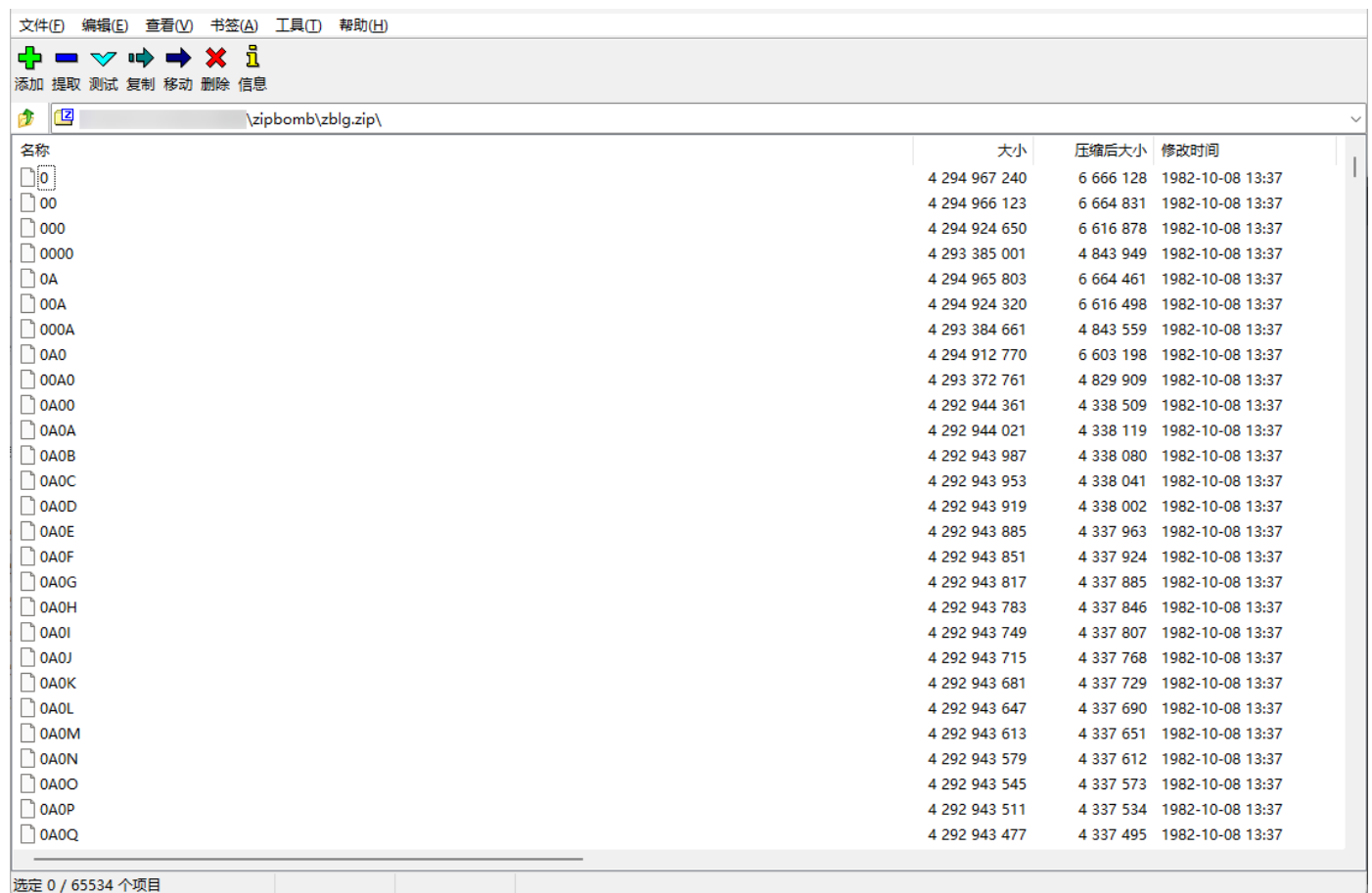
4. 复现步骤

- 后台-->AI大模型-->AI知识库-->文档库上传

点击文档库上传



上传 zblg.zip ，它只有不到10mb，但是完整解压之后会释放大约281TB的文件。



请求包：

```
POST /jeecg-boot/airag/knowledge/doc/import/zip HTTP/1.1
Host: localhost:8080
Accept-Language: zh-CN,zh;q=0.9
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryytDVMHncjQgSAuw1
```



Accept: */*

Referer: http://localhost:81/

X-Requested-With: XMLHttpRequest

Origin: http://localhost:81

X-Tenant-Id: 1000

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch

X-Access-Token: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VybmFtZSI6ImFkbWluIiwiaXNhwIjoxNzQ2MD

Accept-Encoding: gzip, deflate

Content-Length: 34876517

```
-----WebKitFormBoundaryytDVMHncjQgSAuw1
```

Content-Disposition: form-data; name="knowId"

1916389175939362818

```
-----WebKitFormBoundaryytDVMHncjQgSAuw1
```

```
Content-Disposition: form-data; name="file"; filename="zblg.zip"
```

Content-Type: application/x-zip-compressed

zip文件二进制信息

```
-----WebKitFormBoundaryytDVMHncjQgSAuw1--
```

[illegible]

效果

上传前后对比

```
root@node1:~  
[root@node1 ~]# df -h /  
文件系统 容量 已用 可用 已用% 挂载点
```

Closed

v3.8.0存在zip Bomb漏洞 #8199



```
/dev/mapper/centos-root 37G 37G 9.4M 100% /  
[root@node1 ~]# |
```

5. 解决建议

建议限制解压缩文件的总大小和目录递归深度，监控异常压缩率，拒绝过高压缩率或超大文件。



zhangdaiscott 2 weeks ago

Member ...

你部署springboot 和 nginx都没设置大小限制？



lem0n817 2 weeks ago

Author ...

你部署springboot 和 nginx都没设置大小限制？

这个zip不到10mb，没有超过10mb的默认限制



zhangdaiscott 2 weeks ago

Member ...

好



jeecgos 2 weeks ago



已修复，待新版发布。



zhangdaiscott closed this as completed 2 weeks ago

Sign up for free

to join this conversation on **GitHub**. Already have an account? [Sign in to comment](#)

Assignees

No one assigned

Labels

No labels

Type

No type

Projects

No projects

Milestone

No milestone

Relationships

None yet

Development



Code with Copilot Agent Mode



No branches or pull requests

Participants

