

关于我

lake2 ,

腾讯安全平台部总监
TSRC/Blade/腾讯蓝军 CEO
安全运营四杰之一
蓝星安全联盟成员

意外之旅

TSRC与xSRC

意外之旅

2012年，TSRC及腾讯漏洞奖励计划创立



2013年，国内互联网企业开始成立SRC (SRC元年)

*SRC问世以来白帽子总共获得奖励 ¥10,000,000



意外之旅

TSRC面向投后企业推出xSRC SaaS (SRC托管服务)

腾讯xSRC SaaS版本

腾讯xSRC SaaS版本是腾讯安全应急响应中心 (TSRC) 面向合作伙伴推出的用于**快速构建企业安全应急响应中心SRC**的开放平台, 合作伙伴仅需简单几步配置即可完成SRC平台构建, 省去了开发、运维的工作量, 能够更好的专注于漏洞奖励和处置、鼓励白帽子报告漏洞等SRC运营工作。

TSRC开源xSRC代码, 企业可以轻松建设自己的SRC

xSRC开源版

作者: Martin Zhou 公布时间: 2019-10-11 最后更新: 2020-07-21
MD5: dd8e7b5f5cb9ee34f4d1503180372e19
👁 12887 ↓ 4831

[下载该工具](#) [订阅升级通知](#) [分享](#)

腾讯xSRC开源版是腾讯安全应急响应中心 (TSRC) 面向合作伙伴推出的安全应急响应中心 (SRC) 建站软件, 软件源代码开放, 可支持合作伙伴轻松构建SRC平台, 省去大量开发运维工作, 并支持个性化功能及页面设置, 企业数据自主掌控, 安全可靠。

使用文档: <https://docs.qq.com/doc/DSExhSGF1SkJUVnBF>



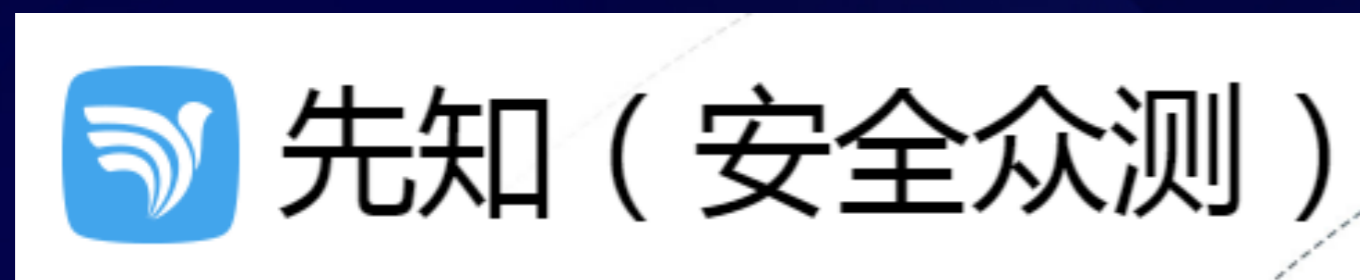
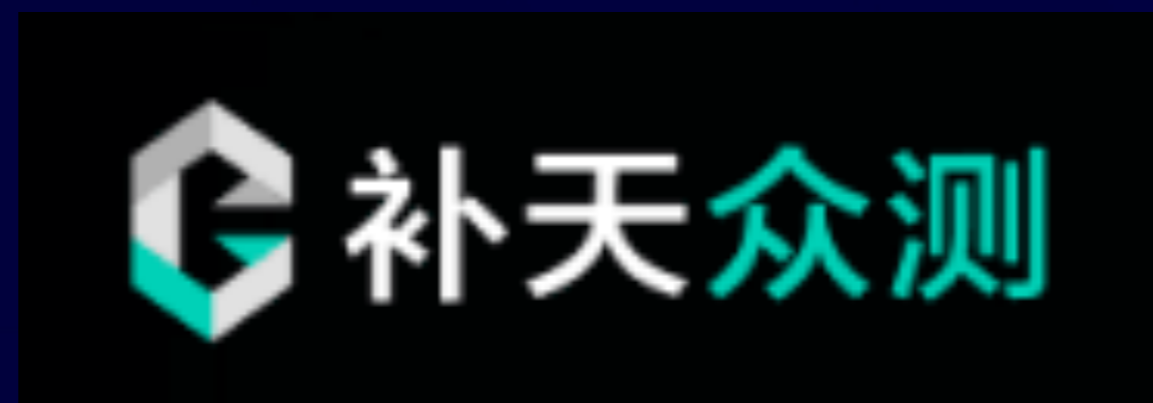
意外之旅

白帽子生态已成



意外之旅

“得白帽者得天下” —— 基于众测的安全服务和产品



云中漫步

云安全产品探索

云中漫步

QQ空间开放平台

开放平台

腾讯云

平台DDoS防护 -> DDoS防护产品

平台HIDS -> HIDS产品

平台WAF -> WAF产品

平台蓝军 -> 红蓝对抗 / 渗透测试 服务

.....

平台系统转商户产品的心酸历程

商户业务架构性能不行

商户业务TCP协议触发防护

其他商户被攻击导致平台抖动

防护系统自身bug

.....

商户业务受到影响

DDoS防护失败

道歉

云中漫步

一些想法

做产业互联网很辛苦

T-Sec DDoS 防护

拥有可信赖的 DDoS 防护体系，可为不同行业提供多种安全解决方案

T-Sec 漏洞扫描服务

便捷、准确的漏洞扫描服务，有效降低企业资产安全风险

T-Sec Web 应用防火墙

基于 AI 的一站式 Web 业务运营风险防护方案，支持多种接入方式

T-Sec 主机安全

提供黑客入侵检测和漏洞监测等安全防护服务

T-Sec 安全专家服务

腾讯云安全专家服务为企业提供安全咨询、渗透测试、应急响应、等保合规等服务

云原生的安全机遇：云原生安全产品 & 云原生的安全 & 安全适配云原生

云中漫步


不赚钱，只是交个朋友

安全能力输出



安全医生

为商户使用微信支付的网站进行安全诊断，并提供诊断说明和修复建议，共建支付安全



产品 解决方案 定价 专栏 帮助与资源 合作

应用安全

WeTest提供应用安全解决方案，模拟黑客攻击，提前探知程序漏洞，进行安全加固，助您提升应用整体安全水平。



【安全通知】PyPI 官方仓库遭遇covd恶意包投毒

作者: 十夜、velora、柯南、腾讯洋葱反入侵系统 发布时间: 2020-11-18 阅读次数: 4504 评论: 4

【安全通知】知名端口转发工具rinetd遭高仿投毒

作者: 柯南、velora、腾讯洋葱反入侵系统 发布时间: 2020-10-09 阅读次数: 510 评论: 0

【安全通知】PyPI 官方仓库遭遇request恶意包投毒

作者: 腾讯洋葱反入侵系统七夜、vspiders、conan 发布时间: 2020-08-05 阅读次数: 4658 评论: 1

天下大同

Tencent Blade Team

天下大同

何为Blade

前沿安全研究团队



AIoT

可信计算

移动设备

基础软件

区块链

云虚拟化

对内：提前规避风险，孵化产品

对外：保护互联网生态，提升影响力

轻用其芒，动即有伤，是为凶器；
深藏若拙，临机取决，是为利器。
——《古剑铭》

天下大同

内部安全保障与业务孵化

腾讯云

产品 解决方案 定价 文档 企业中心 云市场 开发者 支持 合作与生态

可信计算解决方案

利用区块链、可信计算技术，打造数据安全可信共享的基础设施，在保证数据安全和隐私保护的前提下，实现多参与方数据可信共享、协同计算。

立即咨询

报告编号: TS2019IOTS
出具日期: 2019年12月19日

腾讯标准
Tencent Standard

物联网安全等级报告

Tencent
TloT-SEC
三星
钻石级

腾讯物联网安全钻石级

产品名称及版本: 智能门锁

厂商名称: 深圳市 公司

注册地址: 深圳市

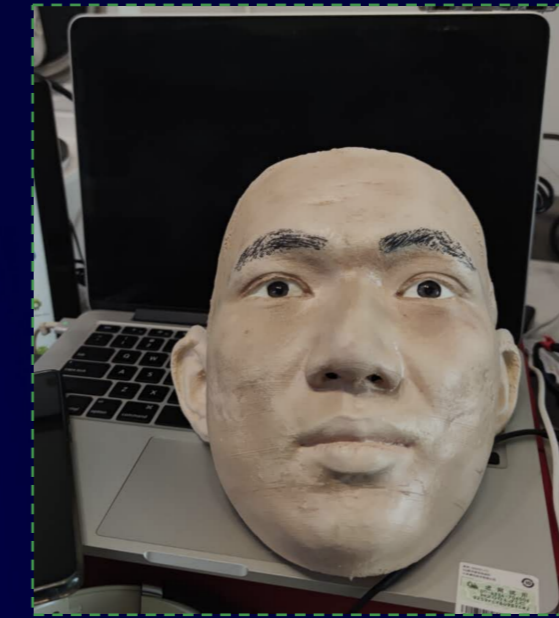
检测机构: 北京银联金卡科技有限公司

上述产品依据腾讯公司技术标准《腾讯物联网安全技术规范 第2部分: 智能门锁安全技术要求》进行测评, 达到钻石级要求。

腾讯云 物联网产品中心

腾讯云

特别声明: 腾讯公司对测评结果的评分作出的等级报告, 腾讯不对检测机构和检测结果的真实性、有效性和准确性承担任何责任。
powered by Tencent Blade Team



NSA方程式组织泄漏文档工具整理与分析

CT

INTERNATIONAL TELECOMMUNICATION UNION
TELECOMMUNICATION STANDARDIZATION SECTOR
STUDY PERIOD 2017-2020

SG20-C643-R1

STUDY GROUP 20
Original: English

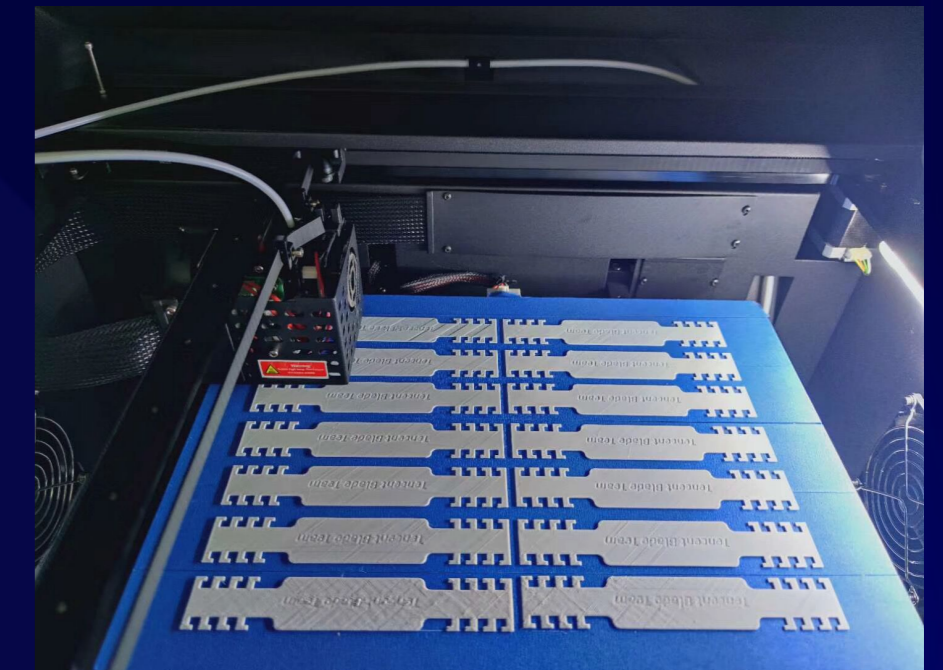
Question(s): 6/20 Geneva, 25 November - 6 December 2019

CONTRIBUTION

Source: Tencent Technology (Shenzhen) Company Limited, China Information Communication Technologies Group (CICT)

Title: Proposal for initiating a new work item on "Requirements of data security for the heterogeneous IoT devices"

Purpose: Proposal



天下大同

为了更安全的互联网

腾讯报告TensorFlow首个安全风险 谷歌确认并致谢

会议	议题名称	研究团队
Black Hat	The Most Secure Browser? Pwning Chrome from 2016 to 2019	Tencent Security Keen Lab
Black Hat	0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars	Tencent Security Keen Lab
Black Hat	Biometric Authentication Under Threat: Liveness Detection Hacking	Tencent Security Xuanwu Lab
Black Hat	Bypassing the Maginat Line: Remotely Exploit the Hardware Decoder on Smartphone	Tencent Blade Team
Black Hat	Battle of Windows Service: A Silver Bullet to Discover File Privilege Escalation Bugs Automatically	Tencent Security Xuanwu Lab
Black Hat	Exploring the New World : Remote Exploitation of SQLite and Curl	Tencent Blade Team
Black Hat	Exploiting Qualcomm WLAN and Modem Over The Air	Tencent Blade Team
DEF CON	Web2Own: Attacking Desktop Apps From Web Security's Perspective	Tencent Security Xuanwu Lab
DEF CON	Breaking Google Home: Exploit it with SQLite(Magellan)	Tencent Blade Team
DEF CON	Your Secret Files Are Mine: Bug Finding And Exploit Techniques On File Transfer App Of All Top Android Vendors	Tencent Security Xuanwu Lab
DEF CON	Exploiting Qualcomm WLAN and Modem Over The Air	Tencent Blade Team

[图]腾讯刀锋安全团队发现严重SQLite漏洞 收到谷歌苹果致谢

2019年12月25日 08:17 4003 次阅读 稿源: cnBeta.COM 1 条评论

近日腾讯刀锋 (Tencent Blade) 安全团队发现了一组名为“Magellan 2.0”的SQLite漏洞, 允许黑客在Chrome浏览器上远程运行各种恶意程序。这组漏洞共有5个, 编号分别为CVE-2019-13734、CVE-2019-13750、CVE-2019-13751、CVE-2019-13752和CVE-2019-13753, 所有使用SQLite数据库的应用均会受到Magellan 2.0攻击影响。

更多相关信息访问: <https://blade.tencent.com/magellan2/index.html>

腾讯刀锋安全团队官方网站: <https://blade.tencent.com/>

LoRaWAN协议栈首个通用漏洞, 可影响全球数亿物联网设备

近日, 全球主流物联网协议LoRa核心技术专利的拥有者、LoRa联盟发起者之一Semtech公司CTO Nicolas Sornin, 专程向腾讯安全平台团队Tencent Blade Team发来感谢信, 致谢其发现并向Semtech报告的LoRaWAN协议栈通用安全漏洞--LoRaDawn, 并期待未来与Tencent Blade Team合作。

据悉, 这也是目前全球首个LoRaWAN协议栈通用漏洞, 影响范围极其广泛。



产品安全通告 > 安全预警

安全预警-浪潮部分服务器BMC未签名校验漏洞

预警编号: INSPUR-SA-202012-001

初始发布时间: 2020-12-04 16:29:28

更新发布时间: 2020-12-04 16:29:28

漏洞来源: 该漏洞由Tencent Blade Team clarkhe上报

漏洞影响: 攻击者可以利用此漏洞控制BMC系统

攻守同盟

蓝军联盟

攻守同盟

实战是检验防护能力的唯一标准

关注安全风险，更要关注安全防御体系的缺陷

不止是渗透，红蓝对抗应该是全方位的

内外部的 Red Team 很重要



攻守同盟

企业蓝军联盟，一起来玩吧



THANKS !

BLADE
Tencent
Blade

 **腾讯蓝军**
Tencent
Force



 **腾讯宙斯盾**
DDoS防护系统

 **TSRC**
腾讯安全应急响应中心

 **K**
金刚系统
KING KONG

ONION^{EDR}
洋葱反入侵系统

 **腾讯铁将军**

 **洞犀**
INSIGHT SCANNER



ICS安全技术峰会

贝壳找房2020 | 产业互联 安全破局