

白帽服务

项目大厅 企业服务

公告活动

攻防社区

冬奥网络安全卫士

提交漏洞

# ios丁香医生app客服聊天存储型超链接xss可任意重定向钓鱼

2022-04-05 13:54:23

 关联厂商:
 丁香园

 奖励额度:
 ¥ 100

 漏洞编号:
 QTVA-2022-2723945

 漏洞类型:
 XSS

 官方评级:
 低危

#### 温馨提示

- 1、已通过的漏洞,定价后将无法查看漏洞详情。
- 2、未通过审核的,七天后将无法查看漏洞详情。

#### 漏洞描述

ios丁香医生app客服聊天存储型超链接xss可任意重定向钓鱼

# 漏洞详情

los丁香医生app

功能点位置: 我的-在线客服(位置在下方)

Payload: 系统提示: <a href=" https://www.baidu.com">点击这里</a > 查看用户留言

payload发过去是这样的

## 漏洞处理状态

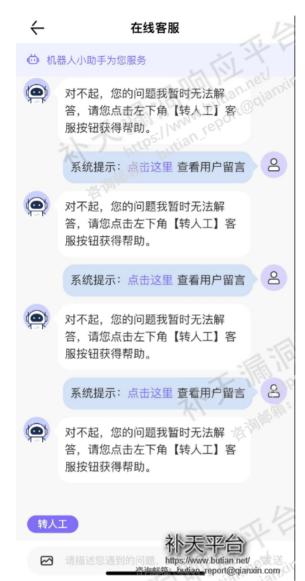
提交漏洞 2022-04-05

被定为事件

奖金确认中

提交漏洞

白帽服务 项目大厅 企业服务 公告活动 攻防社区 冬奥网络安全卫士



点击蓝色字体 直接从app内部转跳到黑客网站,这里以百度为例。

联系人工客服,发送payload可对客服进行钓鱼,因为是app内转跳,迷惑性极强,存在一定危害

白帽服务

项目大厅

企业服务

公告活动 攻防社区 冬奥网络安全卫士

提交漏洞



百度一下





输入搜索词





百度-

#### 时政微视频 | 永远铭记

置顶 央视新闻

一起点亮, 致敬政法英烈!

置顶 环球网

#### 民警为"逆行者"护航

央视新闻



外机逼近, 我战机油量不 足,飞行员果断选择......

"澳被中国海军纳入打击范围!"澳媒鼓吹对所 宣战, 中方务必警惕





## 修复方案

html实体化、html转义

#### 厂商回复

#### 留言板

自古评论出人才, 你也说两句呗

还可以输入120字

给补天留言

# 补天-漏洞\_安全I系统漏洞\_IoTIAPP漏洞\_移动I工控漏洞

白帽服务 项目大厅 企业服务 公告活动 攻防社区 冬奥网络安全卫士 提交漏洞

企业服务 白帽服务 注册热线 商务合作 关注我们

专属SRC 项目大厅 企业咨询: 010-56509036 咨询邮箱: 白帽大会

 补天众测
 白帽众学
 白帽咨询: 010-56509093
 咨询热线: 010-56509055
 官方微博

 安全情报
 补天商城
 咨询邮箱:
 010-56509041
 官方微信

官方4群: 1016907399

官方3群: 774737398 (已满) 官方2群: 320235411 (已满) 官方1群: 322640164 (已满)

友情链接: NOX安全监测 | 奇安信技术研究院 | 奇安信威胁情报中心 | 安全内参

Copyright © 2013-2022 BUTIAN.NET 版权所有 京ICP备18014330号-2

