网络安全创新大会
Cyber Security Innovation Summit

iOS URL Scheme 之殇

Lilang Wu

- Android/macOS/iOS漏洞挖掘和恶意应用分析
  CVE-2016-*, CVE-2018-*, CVE-2019-*
- Android APKs漏洞检测、Exploit检测系统的设计和实现
- Fuzz Project

BH USA 2019, 2018, BH EU 2018, HITB, CodeBlue, VB

Twitter: @Lilang_Wu

- 对App内部资源引用的一种方式
- 能够将App以一种特征上下文的方式打开
- 其它App可以以特定上下文参数打开特定应用

- 自定义自己App的URL数据格式
  - myphotoapp:albumname?name=”albumname”
- 注册到项目的info.plist中
- 重写接收到URL Scheme访问的Handle函数

iOS URL Scheme Warning

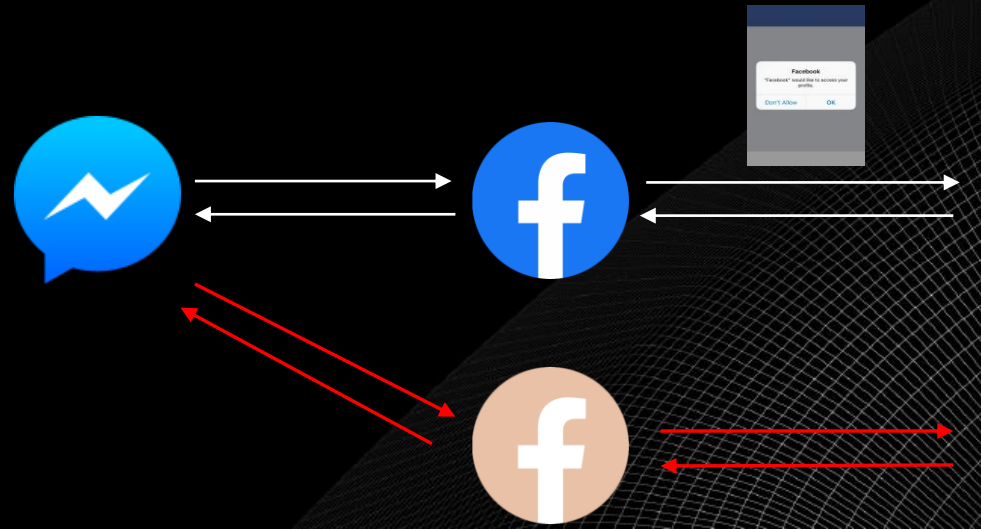
Warning

URL schemes offer a potential attack vector into your app, so make sure to validate all URL parameters and discard any malformed URLs. In addition, limit the available actions to those that do not risk the user's data. For example, do not allow other apps to directly delete content or access sensitive information about the user. When testing your URL-handling code, make sure your test cases include improperly formatted URLs.

https://developer.apple.com/documentation/uikit/inter-process_communication/allowing_apps_and_websites_to_link_to_your_content/defining_a_custom_url_scheme_for_your_app

造成系统层面的漏洞

威胁1 – 账户威胁 - CVE-2016-7651



威胁1 - 漏洞提交

2016/7/31 (周日) 13:41

Lilang Wu (RD-CN)

iOS Privacy and Account Info Leagage Attack

To 'product-security@apple.com'

Cc

You forwarded this message on 2017/12/13 15:50.
This message was sent with High importance.

Dear Apple Security Team

This is Ju Zhu and Lilang Wu from TrendMicro mobile threat research team.
Recently during our further threat research, we found the repacked App can successfully bypass IOS privacy protection mechanism, and even
video to demo the attack, where use repacked Facebook as example.
Attack Video Demo:

1. https://www.ssfe.trendmicro.com.cn/PPMTq/IMG_0218.m4v?a=Y0pRBpLB0e8
2. https://www.ssfe.trendmicro.com.cn/PPMTq/IMG_0220.m4v?a=gJ4TDImxZX8
3. https://www.ssfe.trendmicro.com.cn/PPMTq/IMG_0221.m4v?a=uxGQe9V8nEQ

The view has shown the following attack process:

- ***Video 1 install an official Facebook, and can login use the account profile kept in iOS keyChain. For its first login process, iOS pops up t***
  information. And Then, a similar dialog again when Facebook access user contacts. These behaviors are nothing but normal and neces
- ***However, after delete the genuine Facebook, we install a repacked one in video 2. Unexpected things happen, the repacked one can a***
  information. Worse more, it can also access to user's contracts info freely as if it were official one.
- ***Video 3 show the running process when a user installs repacked Facebook former than official one. Though iOS shows warning dialogs***
  contacts info, that likes cheating users themselves.

2016/9/15 (周四) 5:08

product-security@apple.com

RE: iOS Privacy and Account Info Leagage Attack

To ZDI Disclosures Mailbox; Lilang Wu (RD-CN)

You replied to this message on 2016/10/8 15:48.
We removed extra line breaks from this message.

Please include the line below in follow-up emails for this request.

Follow-up: 645081680

Hello Lilang,

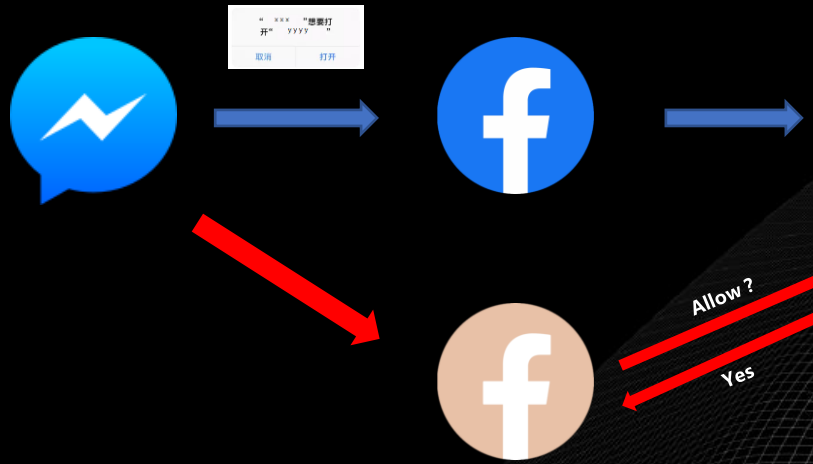
As mentioned previously, we are aware of issue 2 and are still investigating it.

It is an architectural issue and requires the level of effort that goes into a comprehensive fix.

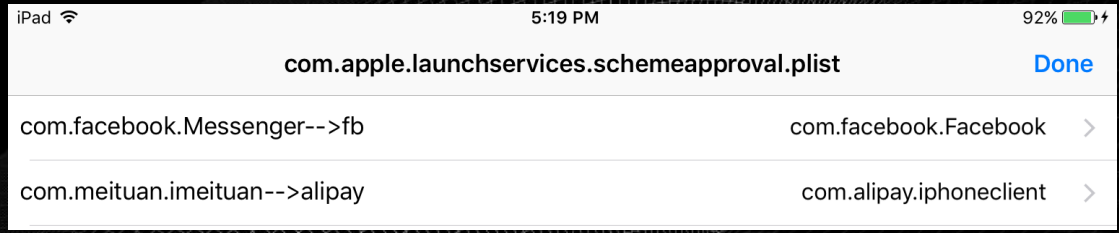
Thank you for working with us as we address the issues you have reported.

Best regards,
Chaitanya
Apple Product Security

威胁2 – Repack or Fake



相同Bundle ID的Repack应用



威胁2 –漏洞提交

2016/8/16 (周二) 20:00

Lilang Wu (RD-CN)

attack channel through sheme

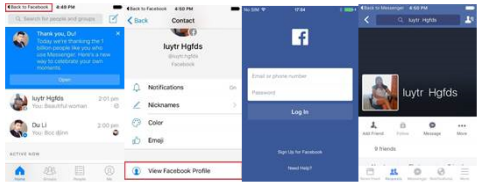
To 'product-security@apple.com'

Cc

You forwarded this message on 2017/12/13 15:49.
This message was sent with High importance.

Hi there,
This is Ju Zhu and Lilang Wu from TrendMicro mobile threat research team.

Recently during our iOS threat research, we found one repacked Facebook apps signed by an enterpri
the attack and also illustrate the attack progress as below:
Attack Video Demo:
https://www.ssfe.trendmicro.com.cn/PPMTq/IMG_01951.mkv?a=_W_nZh95l9g
https://www.ssfe.trendmicro.com.cn/PPMTq/IMG_01921.mkv?a=WOTSu7a4Z6Q



(a) (b) (c) (d)

Steps (a)(b)(c)(d) show the genuine Facebook messenger we installed from iTunes Store wants to view

2016/8/20 (周六) 4:13

product-security@apple.com

Re: attack channel through sheme

To Lilang Wu (RD-CN)

You replied to this message on 2016/9/8 14:29.
We removed extra line breaks from this message.

Please include the line below in follow-up emails for this request.

Follow-up: 646076812

Hello Ju and Lilang,

As usual, thank you for reaching out to us.

In iOS 9, we modified the way URL schemes are handled. The first time an app is c

If a URL scheme is already registered by an app, another app cannot override the UI

Do you agree that this mitigates the threat of a malicious app hijacking the URL sch

Your insights are indeed helpful and thought provoking and we will take them into c

We again thank you for your continuing research and welcome more findings.

Best regards,
Chaitanya Sharma
Apple Product Security

Reply Reply All Forward

2016/10/8 (周六) 8:28

product-security@apple.com

RE: attack channel through scheme

To Lilang Wu (RD-CN)

Cc ZDI Disclosures Mailbox

We removed extra line breaks from this message.

Please include the line below in follow-up emails for this request.

Follow-up: 646076812

Hello Lilang,

Thank you for providing information on the URL scheme association scenario. This is helpful information and we are investigating it.

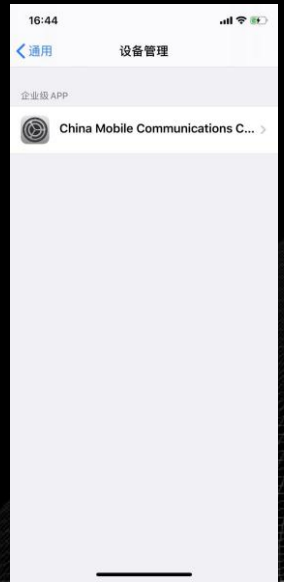
Are you able to confirm that the initial report of an App Store app overriding an enterprise signed app is addressed in the latest

Best regards,
Chaitanya
Apple Product Security

- 用企业证书签Repack Facebook，保持Bundle ID不变
  - CVE-2016-4659 （iOS 10.0），CVE-***
- 让Repack App无感知的覆盖Official App
  - https://support.apple.com/en-us/HT209106 （iOS 12.0）

Refer: https://www.fireeye.com/blog/threat-research/2014/11/masque-attack-all-your-ios-apps-belong-to-us.html

威胁2 – 利用方式

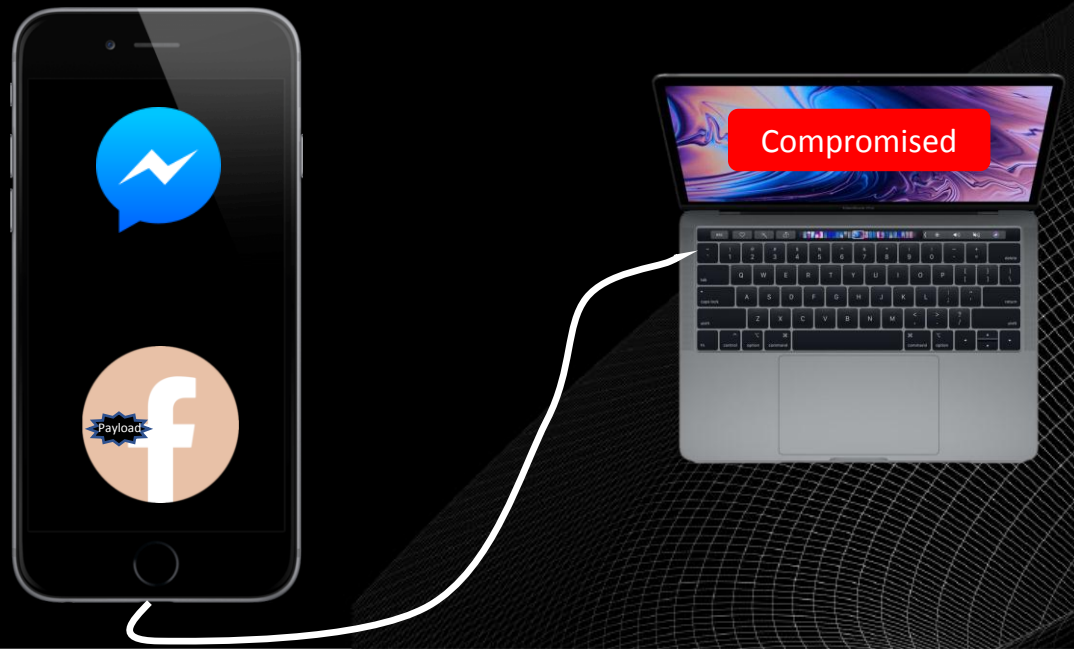



```
mobiledeMacBook-Pro:2019_CIS mobile$ ideviceprovision -h
Usage: ideviceprovision [OPTIONS] COMMAND
Manage provisioning profiles on a device.

 Where COMMAND is one of:
  install FILE  Installs the provisioning profile specified by FILE.
                A valid .mobileprovision file is expected.
  list          Get a list of all provisioning profiles on the device.
  copy PATH     Retrieves all provisioning profiles from the device and
                stores them into the existing directory specified by PATH.
                The files will be stored as UUID.mobileprovision
  copy UUID PATH  Retrieves the provisioning profile identified by UUID
                from the device and stores it into the existing directory
                specified by PATH. The file will be stored as UUID.mobileprovision.
  remove UUID   Removes the provisioning profile identified by UUID.
  remove-all    Removes all installed provisioning profiles.
  dump FILE     Prints detailed information about the provisioning profile
                specified by FILE.

 The following OPTIONS are accepted:
  -d, --debug      enable communication debugging
  -u, --udid UDID  target specific device by UDID
  -x, --xml        print XML output when using the 'dump' command
  -h, --help       prints usage information

Homepage: <http://libimobiledevice.org>
mobiledeMacBook-Pro:2019_CIS mobile$ ideviceprovision list
Device has 10 provisioning profiles installed:
cba1d8d9-9622-46a1-8c9a-b174893e6f55 - GSSV3
64124203-2713-4c1b-8cb3-b88ff72c0685 - iOS Team Provisioning Profile: com.trendmicro.mtrt.CTF-Finals-Mob
954b4505-29c4-47c1-ad60-c7d685c24a88 - iOS Team Provisioning Profile: com.trendmicro.mtrt.TMCTF-Finals
8a532808-8ed2-4978-87fe-36dbab339e9e - iOS Team Provisioning Profile: com.trendmicro.mtrt.test3
c5e82b7e-aedf-4e1b-bdb2-a6c2cd68689a - iOS Team Provisioning Profile: com.trendmicro.mtrt.test2
f746ad5f-c210-4892-8778-6ce4af8b768d - com.cmcc.enterprise-classID.onecardmultinumber.sdk
6e918df0-7e51-4e04-ad3f-819b3c37a6a4 - China Mobile MobileOA made by ZTE for GuangXi
d385bfb6-5d3e-42b0-bd93-13892ea096f7 - iOS Team Provisioning Profile: com.trendmicro.mtrt.test1
bf26fe34-3396-4ab2-9ba2-43e361862096 - iOS Team Provisioning Profile: com.trendmicro.mtrt.adv.CTF-Finals-Mob
0378a463-ec81-4f0d-a394-659e89b1459e - iOS Team Inhouse Provisioning Profile: com.lokfu.replacementhouse
mobiledeMacBook-Pro:2019_CIS mobile$ ideviceprovision remove 6e918df0-7e51-4e04-ad3f-819b3c37a6a4
Profile '6e918df0-7e51-4e04-ad3f-819b3c37a6a4' removed.
mobiledeMacBook-Pro:2019_CIS mobile$
```

威胁2 – 利用方式

- 删除目标手机中的Facebook
- 安装重打包后带有恶意Payload的Facebook（保持Bundle ID 不变）
- 删除企业证书的Provision文件

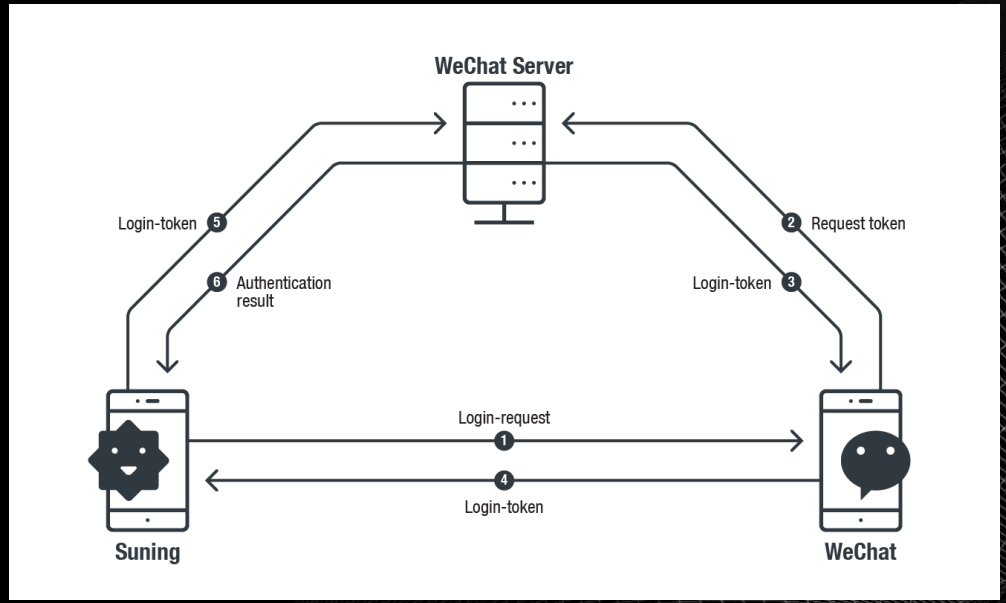
威胁2 – 利用方式



- 删除目标手机中的Facebook
- 安装重打包后带有恶意Payload的Facebook（保持Bundle ID 不变）
- 删除企业证书的Provision文件

造成上层APP的漏洞

威胁3 – 数据劫持 – 微信和苏宁易购为例



- 苏宁易购App请求WeChat认证登录Token的URL Scheme

```
url=====weixin://app/wxe386966df7b712ca/auth/?scope=snsapi_userinfo&state=xxx
```

苏宁注册的用与微信通信的URL Scheme,也就是APPID

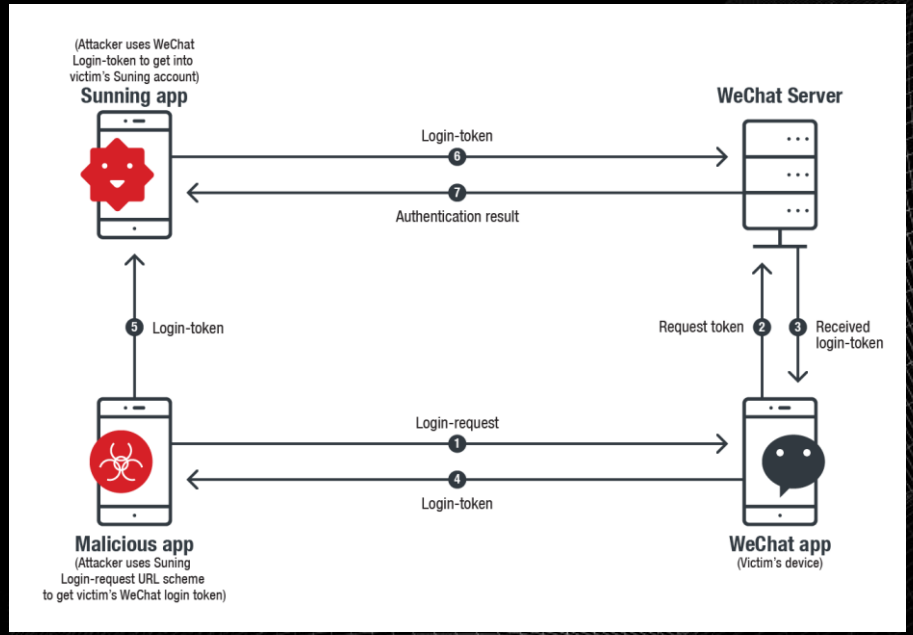
- WeChat返回苏宁易购认证登录Token的URL Scheme

```
url=====wxe386966df7b712ca://oauth?code=02108kz80sbirH1HBcz80rmvz8008kzb&state=xxx
```

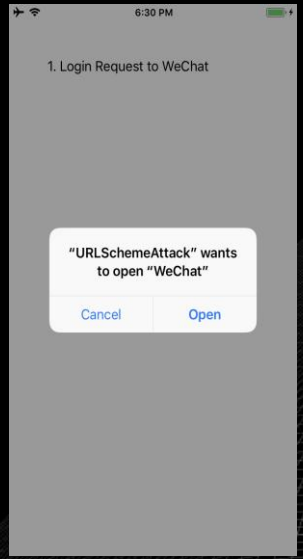
Authentication Code

- 不同Bundle ID APP的URL Scheme特性：
  - iOS 11.0 之前的版本
    - 同一个URL Scheme可以被任意多个App声明和使用
  - iOS 11.0及之后的版本
    - 同一个URL Scheme遵循first-come-first-served的原则

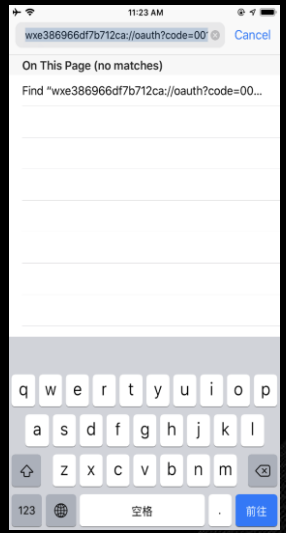
威胁3 – 数据劫持 – 利用方式

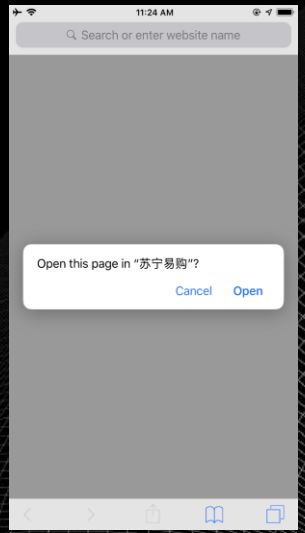


威胁3 – 数据劫持 – 利用方式



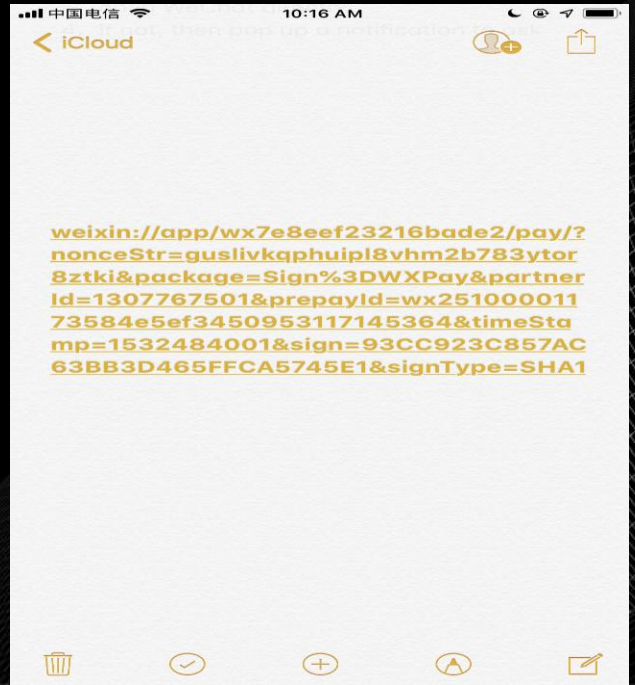
威胁3 – 数据劫持 – 利用方式



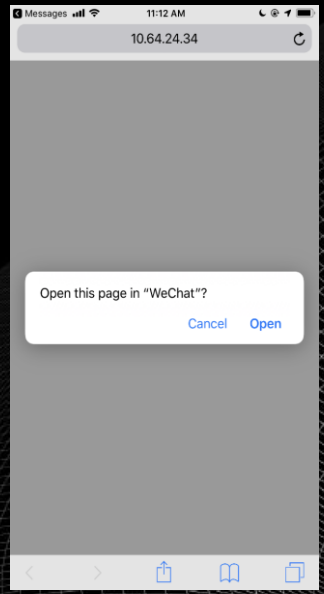


- 方式一：绑卡消费
- 方式二：生成账单
  手动支付

威胁4 - 账单欺诈


中国电信
10:16 AM
iCloud
weixin://app/wx7e8eef23216bade2/pay/?nonceStr=guslivkqphuipl8vhm2b783ytor8ztki&package=Sign%3DWXPay&partnerId=1307767501&prepayId=wx25100001173584e5ef3450953117145364&timeStamp=1532484001&sign=93CC923C857AC63BB3D465FFCA5745E1&signType=SHA1

威胁4 - 账单欺诈 – 利用方式



威胁4 – 漏洞提交

AFFECTED VENDORS	Tencent
AFFECTED PRODUCTS	Wechat
VULNERABILITY DETAILS	This vulnerability allows local attackers to modify requests on vulnerable installations of Tencent WeChat. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of URL schemes. The issue resides in the improper validation if a URL Scheme was acted upon by a malicious application. An attacker can leverage this vulnerability to steal tokens and manipulate requests in the context of current user.
ADDITIONAL DETAILS	This issue was resolved and fixed on the server side. Hence, no patch version number is available.
DISCLOSURE TIMELINE	2018-07-30 - Vulnerability reported to vendor 2019-02-28 - Coordinated public release of advisory

威胁4 – 漏洞提交

AFFECTED PRODUCTS	Alipay
VULNERABILITY DETAILS	This vulnerability allows local attackers to modify requests on affected installations of Alibaba Alipay. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of URL schemes. The issue resides in the improper validation if a URL Scheme was acted upon by a malicious application. An attacker can leverage this vulnerability to steal tokens and manipulate requests in the context of current user.
ADDITIONAL DETAILS	This vulnerability is being disclosed publicly without a patch due to lack of vendor response. 08/31/18 - ZDI reported vulnerability to vendor 01/25/19 - ZDI contacted vendor requesting a status update 01/27/19 - Vendor replied stating they had missed it and requested to send it again. 01/29/19 - ZDI notified the vendor the report would be sent again. 03/07/19 - ZDI contacted vendor requesting a status update 04/01/19 - ZDI contacted vendor requesting a status update and confirmed the case would be published as 0-day. 06/25/19 - ZDI notified vendor the case would be published as 0-day on June 27th. -- Mitigation: Given the nature of the vulnerability the only salient mitigation strategy is to restrict interaction with the application to trusted files.

- 周禹辰

联系我：

- 574407955@qq.com
- 微信：574407955


CIS
网络安全创新大会
Cyber Security Innovation Summit
THANKS