Hacking into iOS's

VoLTE

implementation

Hardik Mehta &

Rajanish Pathak

About Us

Hardik Mehta

@hardw00t

Lead Security Researcher

KATIM

Rajanish Pathak

@h4ckologic

Software Security Researcher

KATIM

Agenda

Introduction

Our Setup

What, How and Why

Q & A

Attack Surfaces

Attack PoC

Disclosure timeline
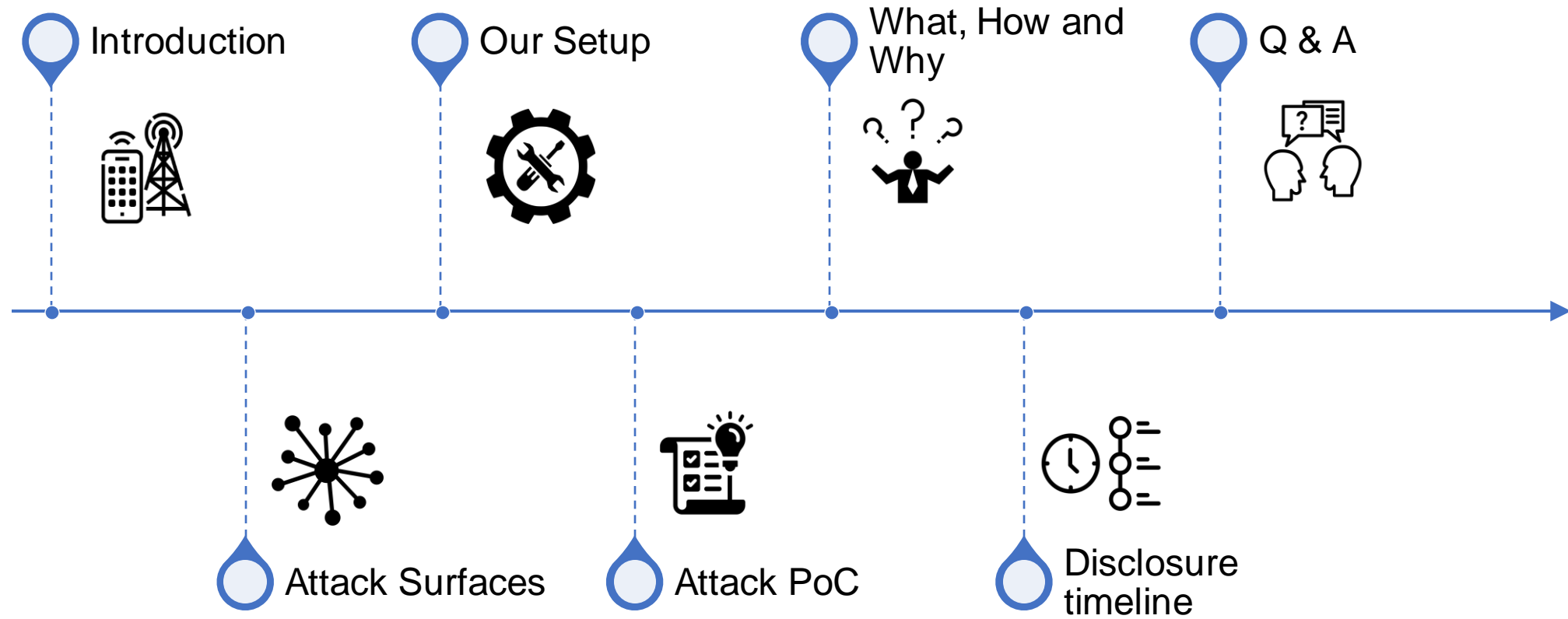
Introduction – Glossary

| Abbreviations	Functions
RAN	Radio Access Network is the part of a mobile network that connects user devices to the core network through base stations, facilitating wireless communication.
EPC	Evolved Packet Core is the core element in LTE networks that manages data traffic, authentication, and mobility for both voice and data services.
HSS	Home Subscriber Server is a centralized database in the networks that stores subscriber information, facilitating authentication, authorization, and mobility management.
MME	Mobility Management Entity is responsible for tracking and managing the mobility of user devices as they move within the network.
SGW	Serving Gateway is used for routing and forwarding user data packets between the mobile device and external networks.
PGW	Packet Data Network Gateway is used to manage data routing and connectivity between the network and external packet data networks, such as the Internet and IMS.
IMS	IP Multimedia Subsystem enables the delivery of multimedia services, including VoLTE, over IP networks with separation of control and media planes.
CSCF	Call Session Control Function is a component in the IMS architecture that controls the signalling and setup of multimedia sessions, including VoLTE calls.

Introduction – LTE/ 5G (NSA) Architecture
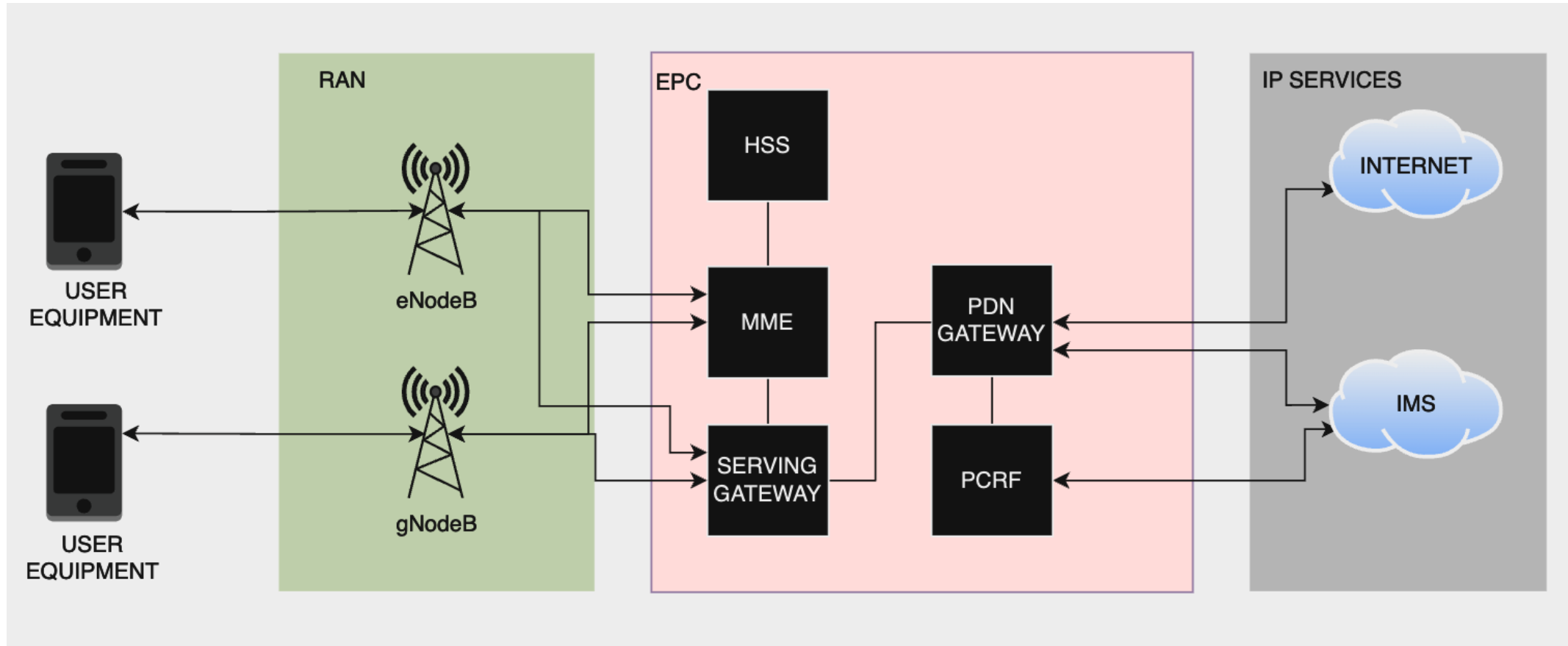
Introduction – VoLTE Architecture

- VoLTE relies on the IMS for delivering multimedia services over IP networks. IMS separates the control plane (call setup and signalling) from the media plane (voice and data transmission).
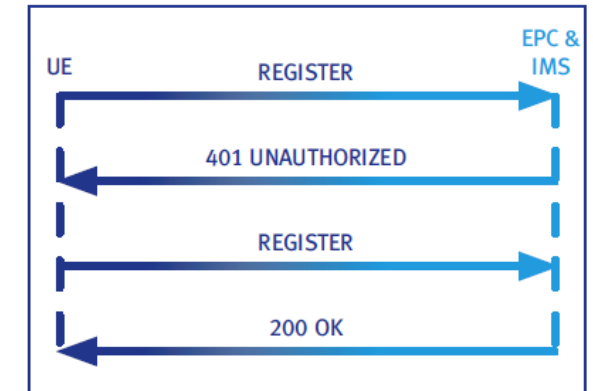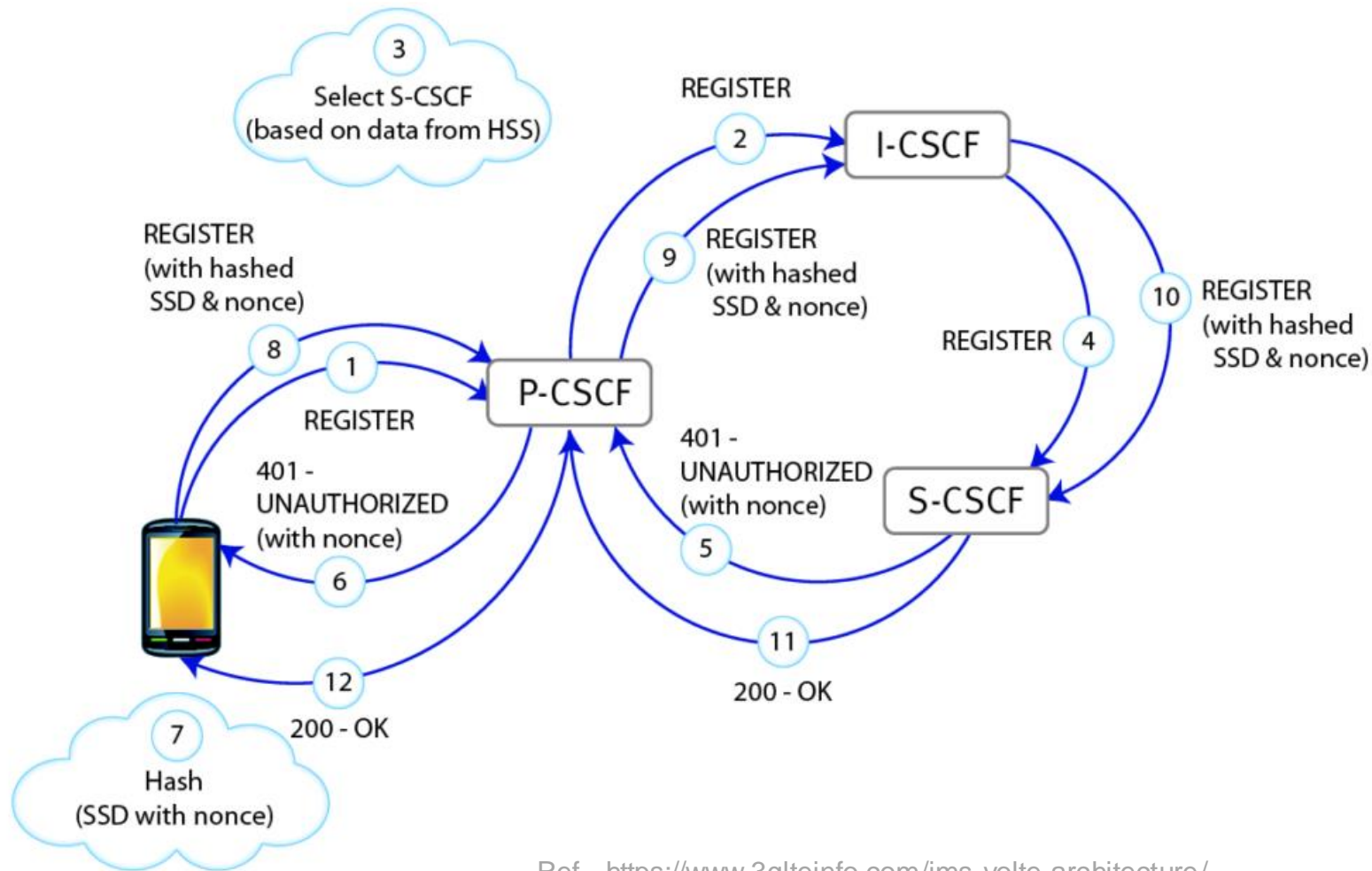
- The EPC serves as the backbone for VoLTE calls.
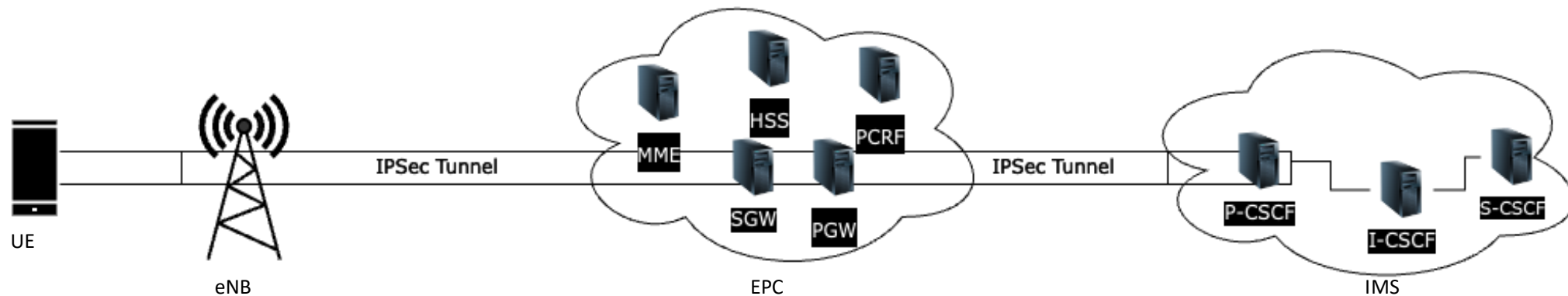
Introduction – VoLTE Protocols

- SIP: Used for call setup, modification, and termination.

- SDP: Describes the multimedia content of a session.

- RTP: Carries the actual voice media during the call.

- RTCP: Provides control and monitoring functions for RTP.

UE

eNB

IPSec Tunnel

MME
HSS
PCRF
SGW
PGW

EPC

IPSec Tunnel

P-CSCF
I-CSCF
S-CSCF

IMS
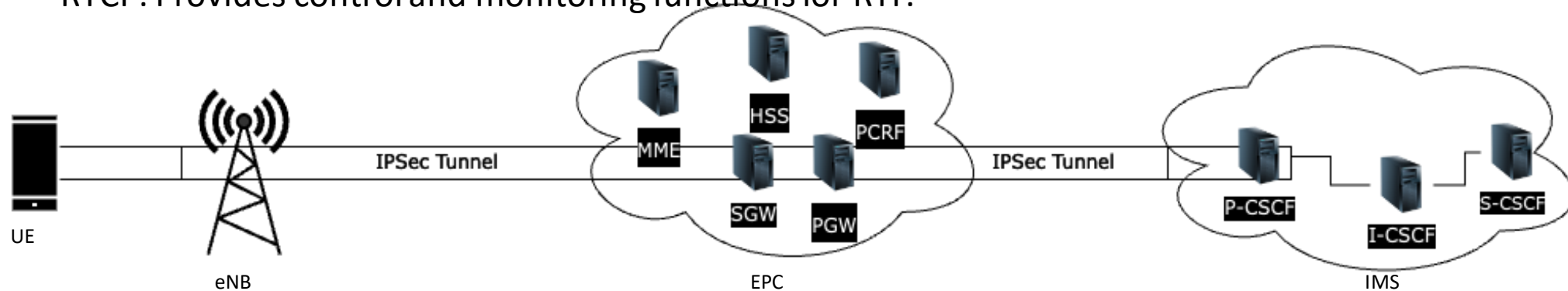
Introduction – VoLTE Registration Flow

Ref - https://www.3glteinfo.com/ims-volte-architecture/

Introduction - Security Issues in VoLTE

- Enumerate services of IMS, EPC and transmission nodes such as aggregation routers, EPDG, UAG / PCSCF

- It is possible to send REGISTER and INVITE SIP requests to identified UAG and CSCF nodes.

- Initiate SIP related attacks like session hijacking, REGISTER and INVITE flooding attacks which introduces a delay and continuous server time-out response

- Targeting other VoLTE users in the network

- Targeting device baseband and fuzzing over SIP protocol
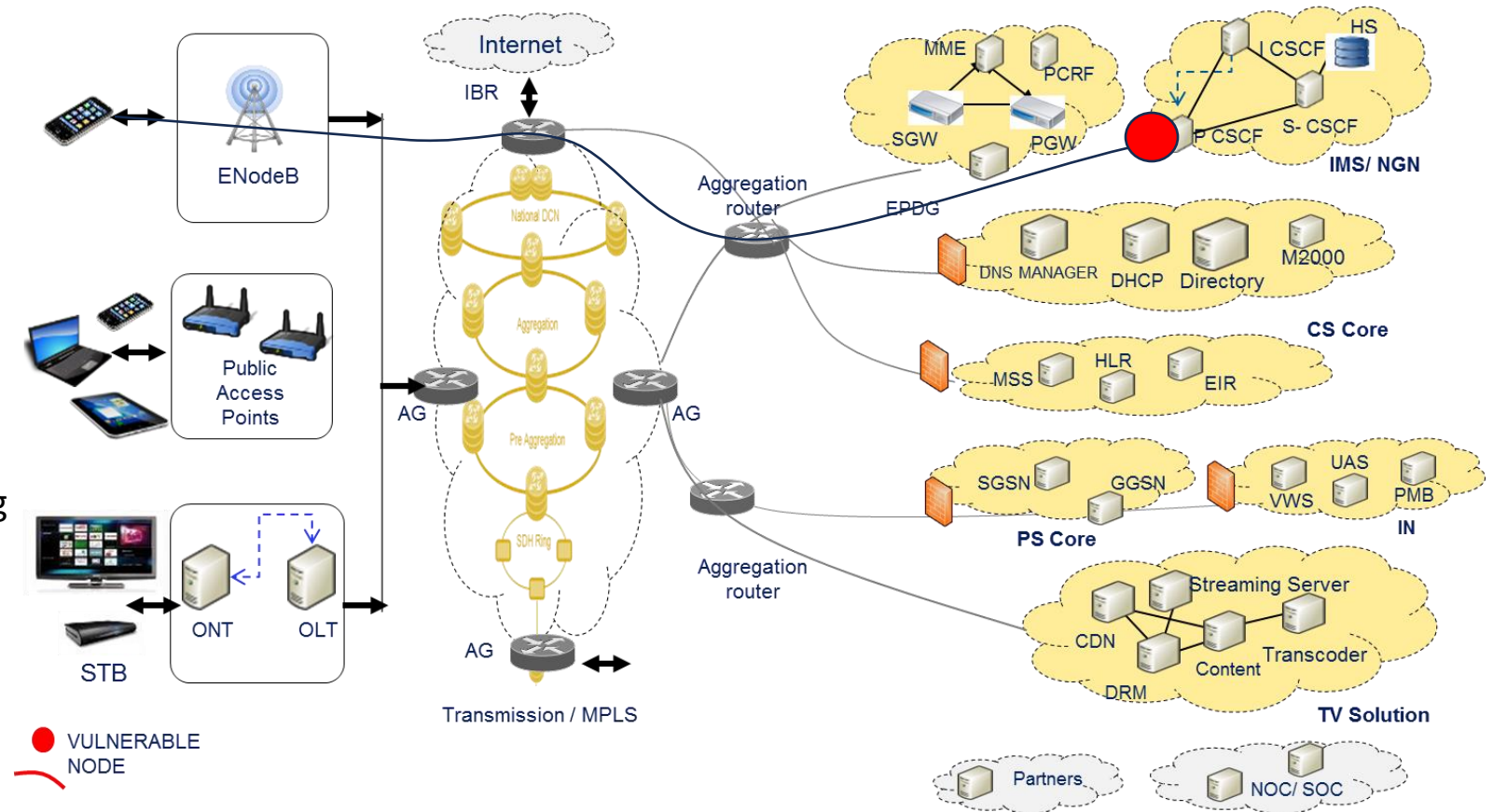
Our Setup

- VoLTE test network using Open5Gs with Kamailio

- SDR - USRP B210 and Bladerf x40

- Test SIMs

- Target iPhone and attacking Android devices

- Attacking Android device is set up working with APN 'ims' only mode

- Traffic routing is done using 'iptables' rules or forwarding the raw packets using 'socat'
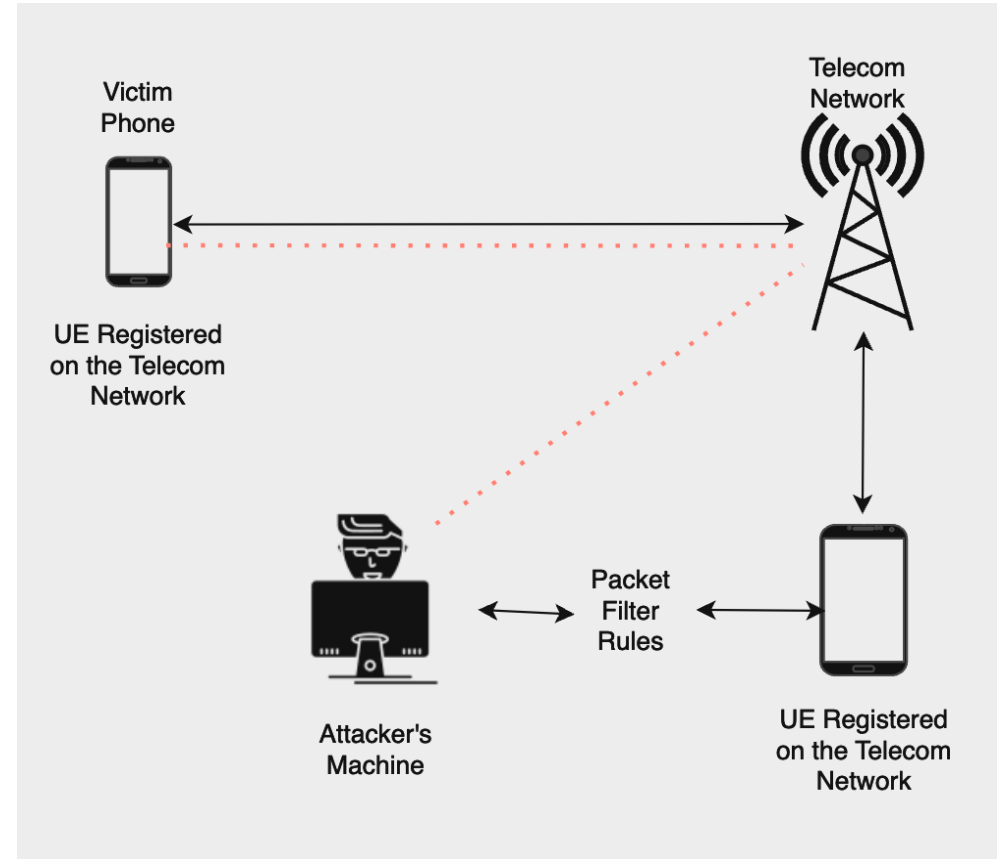
PoC
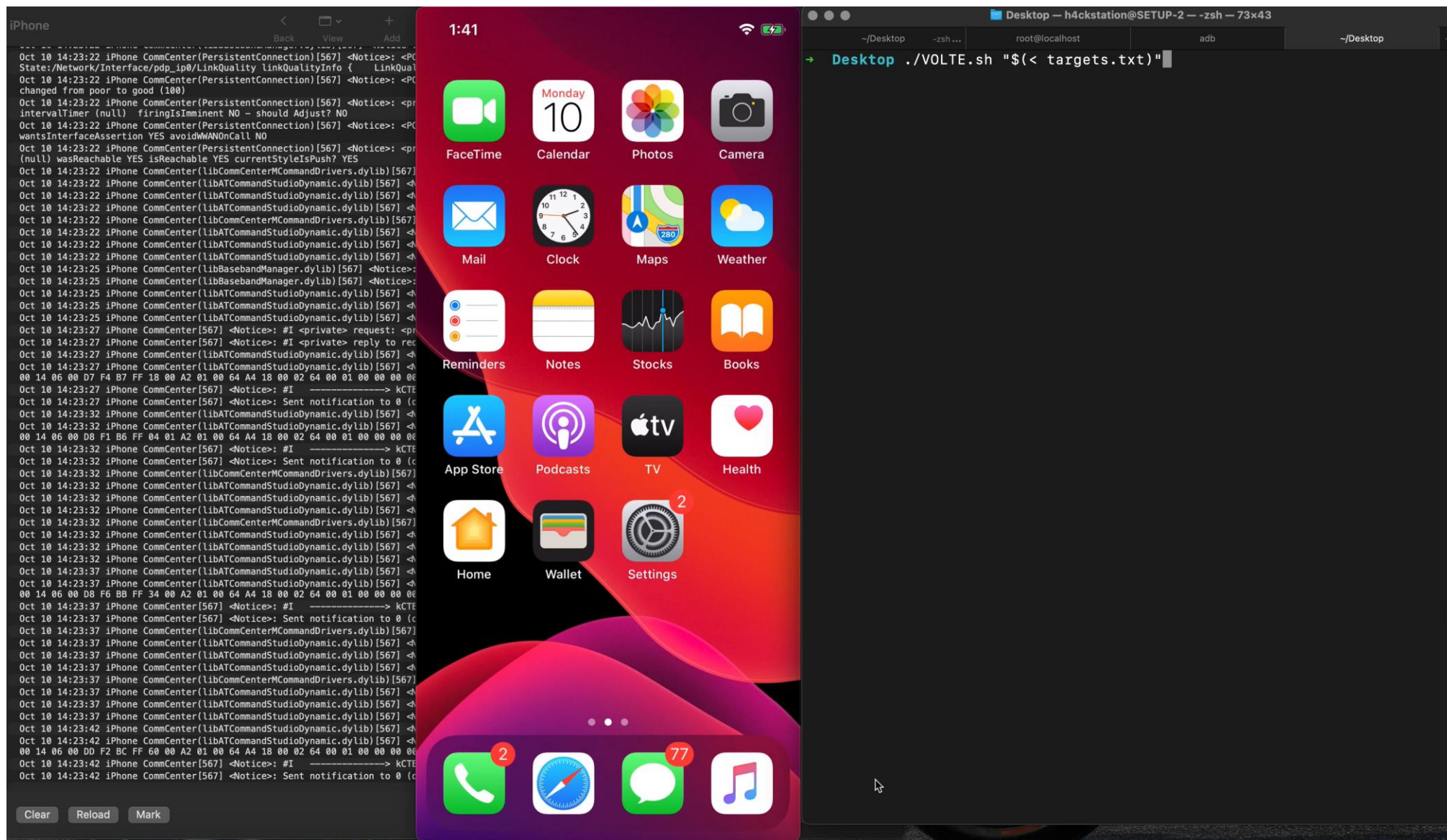
PoC

Using this technique, identified several million iOS devices which are connected on the VoLTE network

```
+-----------------------+--------------------------------+
| SIP Device            | User Agent                     |
+=======================+================================+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/13.2 (17B84) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.3 (18C66) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/12.4 (16G77) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.0 (18A5342e) iPhone      |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
| 10.168        5060    | iOS/14.4 (18D52) iPhone         |
+--------      -------+--------------------------------+
```

Impact

- **Enumeration**: Enumeration of iOS devices in the LTE network with iOS version to launch targeted attack.
- **PII**: Attacker can get access to critical PII information about the subscriber, like MSISDN, IMEI and phone OS version.

- **Spoofing**: Attacker may use PII information for various malicious purposes like, spoofing, spamming and fraud.
- **Dos**: Attacker may exhaust user equipment with malformed SIP packet making it difficult for the subscribers to make or answer calls.

- **Network congestion:** Attacker may amplify the attack by sending random INVITE packets to all the identified iOS devices, this will make all the devices ring with incoming calls leading to network congestion.
- Further, attacker can perform SIP related attacks including fuzzing, targeting exposed SIP interface of the devices.

What, How and Why?

Vulnerability Identification – iOS internals

- As soon as the Airplane mode was turned off the interface (pdp_ip1) is brought online.
- Security policies for pdp_ip1 were updated
- Ipv4 assignment is carried out

```
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: Interface pdp_ip1: mtu 1450
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]:    100.65.13.96
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]:
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: looking for a local IP4 address on pdp_ip1 to contact 10.225.50.20
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: found IP4 address 100.65.13.96 on pdp_ip1
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: pdp_ip1 is already up
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: state transition [WaitingForInterface --> WaitingForReachability]
May  3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17171] DNSServiceCreateConnection START PID[392](apsd)
May  3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17172] DNSServiceGetAddrInfo(C000D000, 2, 0, <private>) START PID[392](apsd)
May  3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17172->Q56438] GetServerForQuestion: 0x101813600 DNS server (0x100c06e90) <private>:53 (Penalty Time Left 0) (Scope pdp_ip0:0x2:-1) for <private> (
AAAA)
May  3 02:25:29 Rajanishs-iPhone mDNSResponder[404] <Notice>: [R17172->Q55283] GetServerForQuestion: 0x101829600 DNS server (0x100c06e90) <private>:53 (Penalty Time Left 0) (Scope pdp_ip0:0x2:-1) for <private> (
Addr)
```

Vulnerability Identification – iOS internals

- The default socket for SIP i.e port 5060 is opened and assigned to pdp_ip1

- The device initiates the registration process over the IMS by sending the REGISTER packet utilizing port 5060.

```
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: binding IPv4 socket to interface pdp_ip1 (index 3)
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: ImsUdpSocket 0x0x1358919f0: added runloop source for CFSocket 0x0x13599b2c0
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: kCFSocketCloseOnInvalidate flag is on by default
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set UUID 67A03811-DB0A-594E-C2AE-8B0517EDF26F on socket fd=35
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set IP_TOS on IPv4 socket fd=35
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set SO_TRAFFIC_CLASS on socket fd=35
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: InsecureTransport [Uninitialized]: Using 5060 port as TCP source port
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: binding IPv4 socket to interface pdp_ip1 (index 3)
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: ImsListenSocket 0x0x13587c120: added runloop source for CFSocket 0x0x135869b60
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: kCFSocketCloseOnInvalidate flag is on by default
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set UUID 67A03811-DB0A-594E-C2AE-8B0517EDF26F on socket fd=36
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set IP_TOS on IPv4 socket fd=36
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: Set SO_TRAFFIC_CLASS on socket fd=36
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: SipTcpTransport: outgoing connections will use port 5060
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: initialized transport InsecureTransport [100.65.13.96:5060]
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: state transition [InitializingTransport --> Idle]
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: TransportLayer: notifying delegate of transport initialization with result Bambi: Success
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.reg]: RegistrationClient: state transition [InitializingTransport --> SendingInitialRequest]
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [sip.tport]: IPSecTransport [0 --> 0, 0 <-- 0]: SipIPSecTransportGroup::initialize()
May  3 02:25:29 Rajanishs-iPhone CommCenter(libIPTelephony.dylib)[368] <Notice>: [net]: binding IPv4 socket to interface pdp_ip1 (index 3)
```

Vulnerability Identification – iOS internals

- The device initiates the registration process over the IMS by sending the REGISTER packet utilizing port 5060.

Vulnerability Identification – iOS internals

- The registration over 5060 fails with status 401 and a process for secure connection over IPSec is initiated

Vulnerability Identification – iOS internals

- But the socket connection on 5060 is left as it is and it still continues to listen for incoming SIP traffic.

```
Rajanishs-iPhone:~ root# lsof -i
COMMAND       PID        USER    FD   TYPE             DEVICE SIZE/OFF   NODE NAME
launchd       1          root    8u   IPv6 0x32fd9b4111b2b3df     0t0    TCP localhost:intu-ec-client (LISTEN)
launchd       1          root    10u  IPv4 0x32fd9b4111b453a7     0t0    TCP localhost:intu-ec-client (LISTEN)
launchd       1          root    12u  IPv4 0x32fd9b4111265957     0t0    TCP localhost:socks (LISTEN)
launchd       1          root    13u  IPv4 0x32fd9b411126630f     0t0    TCP localhost:ansoft-lm-1 (LISTEN)
launchd       1          root    14u  IPv6 0x32fd9b4111b2adbf     0t0    TCP *:62078 (LISTEN)
launchd       1          root    15u  IPv4 0x32fd9b4111266cc7     0t0    TCP *:62078 (LISTEN)
launchd       1          root    17u  IPv6 0x32fd9b4111b2a79f     0t0    TCP *:ssh (LISTEN)
launchd       1          root    18u  IPv4 0x32fd9b411126767f     0t0    TCP *:ssh (LISTEN)
launchd       1          root    20u  IPv6 0x32fd9b4111b2b3df     0t0    TCP localhost:intu-ec-client (LISTEN)
launchd       1          root    21u  IPv4 0x32fd9b4111b453a7     0t0    TCP localhost:intu-ec-client (LISTEN)
launchd       1          root    22u  IPv4 0x32fd9b4111f868bf     0t0    TCP localhost:7808 (LISTEN)
launchd       1          root    24u  IPv4 0x32fd9b4111265957     0t0    TCP localhost:socks (LISTEN)
launchd       1          root    25u  IPv4 0x32fd9b411126630f     0t0    TCP localhost:ansoft-lm-1 (LISTEN)
launchd       1          root    27u  IPv4 0x32fd9b41186753a7     0t0    TCP localhost:ssh->localhost:63345 (ESTABLISHED)
launchd       1          root    28u  IPv4 0x32fd9b4111f868bf     0t0    TCP localhost:7808 (LISTEN)
launchd       1          root    29u  IPv4 0x32fd9b41186753a7     0t0    TCP localhost:ssh->localhost:63345 (ESTABLISHED)
launchd       1          root    30u  IPv6 0x32fd9b4111b2a79f     0t0    TCP *:ssh (LISTEN)
launchd       1          root    31u  IPv4 0x32fd9b411126767f     0t0    TCP *:ssh (LISTEN)
rapportd      310        mobile  7u   IPv4 0x32fd9b411866fc2f     0t0    TCP 169.254.98.39:63344->hackstation.local:56171 (ESTABLISHED)
configd       319        root    5u   IPv4 0x32fd9b4111b6d26e7    0t0    UDP *:bootpc
configd       319        root    6u   IPv6 0x32fd9b411855ef9f     0t0 ICMPV6 *:*
wifid         330        root    4u   IPv4 0x32fd9b411148acb7     0t0    UDP *:*
wifid         330        root    5u   IPv4 0x32fd9b411148c3f7     0t0    UDP *:*
wifid         330        root    15u  IPv4 0x32fd9b411153e6e7     0t0    UDP *:*
wifid         330        root    17u  IPv4 0x32fd9b411153f857     0t0    UDP *:*
wifid         330        root    19u  IPv4 0x32fd9b411153e3ff     0t0    UDP *:*
identitys     337        mobile  23u  IPv4 0x32fd9b4111427b3f     0t0    UDP *:*
identitys     337        mobile  25u  IPv6 0x32fd9b411231f9ff     0t0    TCP [fe80:12::db21:fadd:a2d5:d964]:1024->[fe80:12::fc89:3398:f417:5220]:1024 (SYN_SENT)
lockdownd     356        root    5u   IPv4 0x32fd9b4111266cc7     0t0    TCP *:62078 (LISTEN)
lockdownd     356        root    6u   IPv4 0x32fd9b4111b2adbf     0t0    TCP *:62078 (LISTEN)
frida-ser     363        root    7u   IPv4 0x32fd9b4111b405e7     0t0    TCP localhost:27042 (LISTEN)
frida-ser     363        root    13u  IPv6 0x32fd9b4111b2c63f     0t0    TCP *:49435 (LISTEN)
CommCente     368        _wireless  35u  IPv4 0x32fd9b4113019567  0t0    UDP 100.65.13.96:sip
CommCente     368        _wireless  36u  IPv4 0x32fd9b411867230f  0t0    TCP 100.65.13.96:sip (LISTEN)
CommCente     368        _wireless  37u  IPv4 0x32fd9b4111b6d2cb7  0t0    UDP 100.65.13.96:53852
CommCente     368        _wireless  40u  IPv4 0x32fd9b41136d29cf   0t0    UDP 100.65.13.96:54700
CommCente     368        _wireless  41u  IPv4 0x32fd9b4118672cc7   0t0    TCP 100.65.13.96:54700 (LISTEN)
CommCente     368        _wireless  42u  IPv4 0x32fd9b4118635f07   0t0    TCP 100.65.13.96:53852 (LISTEN)
CommCente     368        _wireless  45u  IPv4 0x32fd9b411863d3a7   0t0    TCP 100.65.13.96:54700->10.225.50.20:7807 (ESTABLISHED)
apsd          392        mobile  11u  IPv6 0x32fd9b411232127f     0t0    TCP [2001:8f8:1f03:e23c:18c6:1b4c:fd4a:a1ce]:63342->[2403:300:a42:c0a::8]:5223 (ESTABLISHED)
apsd          392        mobile  14u  IPv6 0x32fd9b411232127f     0t0    TCP [2001:8f8:1f03:e23c:18c6:1b4c:fd4a:a1ce]:63342->[2403:300:a42:c0a::8]:5223 (ESTABLISHED)
```

Vulnerability Identification – Android

- Android operating system terminates the socket connection to PORT 5060 if it is not being utilized it can be seen from the logs below.

PoC

1. Identification of iOS devices on the network.

PoC

2. Sending crafted SIP INVITE packet to confirm remote device is responding to incoming SIP request

PoC

3. Trace captured on Wireshark where the device accepts incoming traffic and the call is initiated.

PoC

4. The iOS device still continues to listen on SIP port 5060 despite an already established and serving call session

```
[iPhone:~ root# lsof -Pnl +M -i4
COMMAND      PID   USER   FD   TYPE     DEVICE SIZE/OFF NODE NAME
launchd        1      0    9u   IPv4 0x35c060e9ace9463      0t0  TCP 127.0.0.1:8021 (LISTEN)
launchd        1      0   12u   IPv4 0x35c060e962e4eb3      0t0  TCP 127.0.0.1:1080 (LISTEN)
launchd        1      0   13u   IPv4 0x35c060e962e00f3      0t0  TCP 127.0.0.1:1083 (LISTEN)
launchd        1      0   15u   IPv4 0x35c060e962e3b43      0t0  TCP *:62078 (LISTEN)
launchd        1      0   17u   IPv4 0x35c060e95c6ed83      0t0  TCP 127.0.0.1:7808 (LISTEN)
launchd        1      0   20u   IPv4 0x35c060e9ace9463      0t0  TCP 127.0.0.1:8021 (LISTEN)
launchd        1      0   21u   IPv4 0x35c060e95c6ed83      0t0  TCP 127.0.0.1:7808 (LISTEN)
launchd        1      0   23u   IPv4 0x35c060e962e4eb3      0t0  TCP 127.0.0.1:1080 (LISTEN)
launchd        1      0   24u   IPv4 0x35c060e962e00f3      0t0  TCP 127.0.0.1:1083 (LISTEN)
launchd        1      0   26u   IPv4 0x35c060e962de3cb      0t0  TCP *:22 (LISTEN)
launchd        1      0   28u   IPv4 0x35c060e962de3cb      0t0  TCP *:22 (LISTEN)
launchd        1      0   30u   IPv4 0x35c060e98ea40f3      0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
launchd        1      0   31u   IPv4 0x35c060e98ea40f3      0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
configd     1522      0   18u   IPv4 0x35c060e95ff62f3      0t0  UDP *:68
wifid       1533      0    4u   IPv4 0x35c060e9803374b      0t0  UDP *:*
wifid       1533      0    5u   IPv4 0x35c060e9803317b      0t0  UDP *:*
wifid       1533      0   15u   IPv4 0x35c060e95ff8ba3      0t0  UDP *:*
wifid       1533      0   17u   IPv4 0x35c060e95ff85d3      0t0  UDP *:*
wifid       1533      0   19u   IPv4 0x35c060e95ff8003      0t0  UDP *:*
identitys   1540    501   23u   IPv4 0x35c060e95ff1a2b      0t0  UDP *:*
lockdownd   1558      0    5u   IPv4 0x35c060e962e3b43      0t0  TCP *:62078 (LISTEN)
CommCente   1570     25   37u   IPv4 0x35c060e9af3c5d3      0t0  UDP 10.165.172.172:5060
CommCente   1570     25   38u   IPv4 0x35c060e99dbbb43      0t0  TCP 10.165.172.172:5060 (LISTEN)
CommCente   1570     25   39u   IPv4 0x35c060e9af3c8bb      0t0  UDP 10.165.172.172:49998
CommCente   1570     25   40u   IPv4 0x35c060e9af3cba3      0t0  UDP 10.165.172.172:53295
CommCente   1570     25   41u   IPv4 0x35c060e99db9463      0t0  TCP 10.165.172.172:53295 (LISTEN)
CommCente   1570     25   42u   IPv4 0x35c060e9acbd463      0t0  TCP 10.165.172.172:49998 (LISTEN)
CommCente   1570     25   47u   IPv4 0x35c060e9acbcaab      0t0  TCP 10.165.172.172:53295->10.225.50.148:7807 (ESTABLISHED)
CommCente   1570     25   48u   IPv4 0x35c060e97d6fd1b      0t0  UDP 10.165.172.172:49120
CommCente   1570     25   49u   IPv4 0x35c060e97d70ba3      0t0  UDP 10.165.172.172:49121
apsd        1594    501   10u   IPv4 0x35c060e98ea7b43      0t0  TCP 10.38.133.66:50524->17.57.145.6:5223 (ESTABLISHED)
apsd        1594    501   12u   IPv4 0x35c060e98ea7b43      0t0  TCP 10.38.133.66:50524->17.57.145.6:5223 (ESTABLISHED)
wifianaly   1602      0    4u   IPv4 0x35c060e97d6ebab      0t0  UDP *:*
mDNSRespo   1609     65    6u   IPv4 0x35c060e95ff7463      0t0  UDP *:5353
companion   1803    501    4u   IPv4 0x35c060e962e0aab      0t0  TCP 127.0.0.1:50395->127.0.0.1:50396 (ESTABLISHED)
notificat   1804    501    5u   IPv4 0x35c060e99d744fb      0t0  TCP 127.0.0.1:50417->127.0.0.1:50418 (ESTABLISHED)
notificat   1804    501    6u   IPv4 0x35c060e98ea4aab      0t0  TCP 127.0.0.1:50455->127.0.0.1:50456 (ESTABLISHED)
notificat   1804    501    7u   IPv4 0x35c060e95c744fb      0t0  TCP 127.0.0.1:50492->127.0.0.1:50493 (ESTABLISHED)
notificat   1804    501    8u   IPv4 0x35c060e99d727d3      0t0  TCP 127.0.0.1:50517->127.0.0.1:50518 (ESTABLISHED)
DTService   1812      0    4u   IPv4 0x35c060e98df23cb      0t0  TCP 127.0.0.1:50439->127.0.0.1:50440 (ESTABLISHED)
frida-ser   4031      0    7u   IPv4 0x35c060e95b9986b      0t0  TCP 127.0.0.1:27042 (LISTEN)
gamed       4702    501    4u   IPv4 0x35c060e97d6ee93      0t0  UDP 10.38.133.66:16403
sshd        4904      0    4u   IPv4 0x35c060e98ea40f3      0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
sshd        4904      0    5u   IPv4 0x35c060e98ea40f3      0t0  TCP 127.0.0.1:22->127.0.0.1:50521 (ESTABLISHED)
```

Root Cause

- VoLTE enabled iOS devices are always listening on interface "pdp_ip1" on Port 5060 irrespective of them being connected with the P-CSCF (IMS) on a different port.

- While the call is established via IMS channel, it is observed the devices continue to listen for incoming SIP traffic.

- Attacker on the operator's network can identify these devices and gain information like, iOS version, IMEI number and MSISDN of the subscriber

- Attacker on the operator's network can make spoof calls directly interacting with the devices itself by crafting malformed SIP packets.
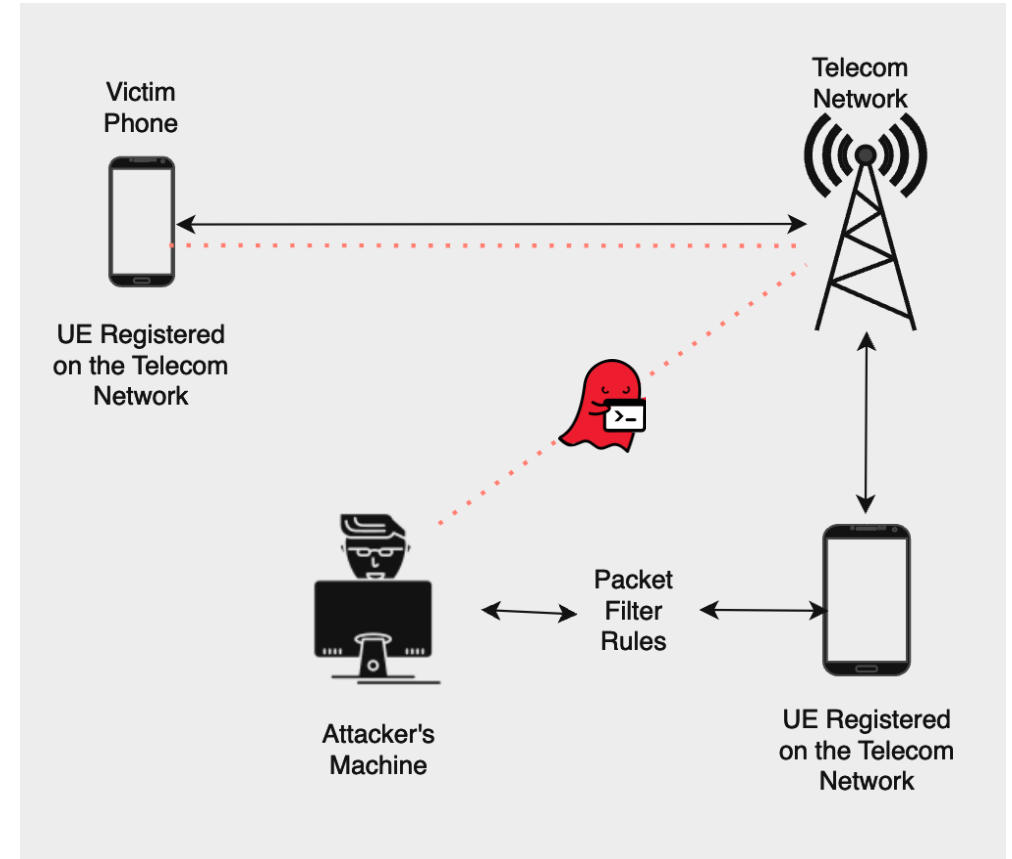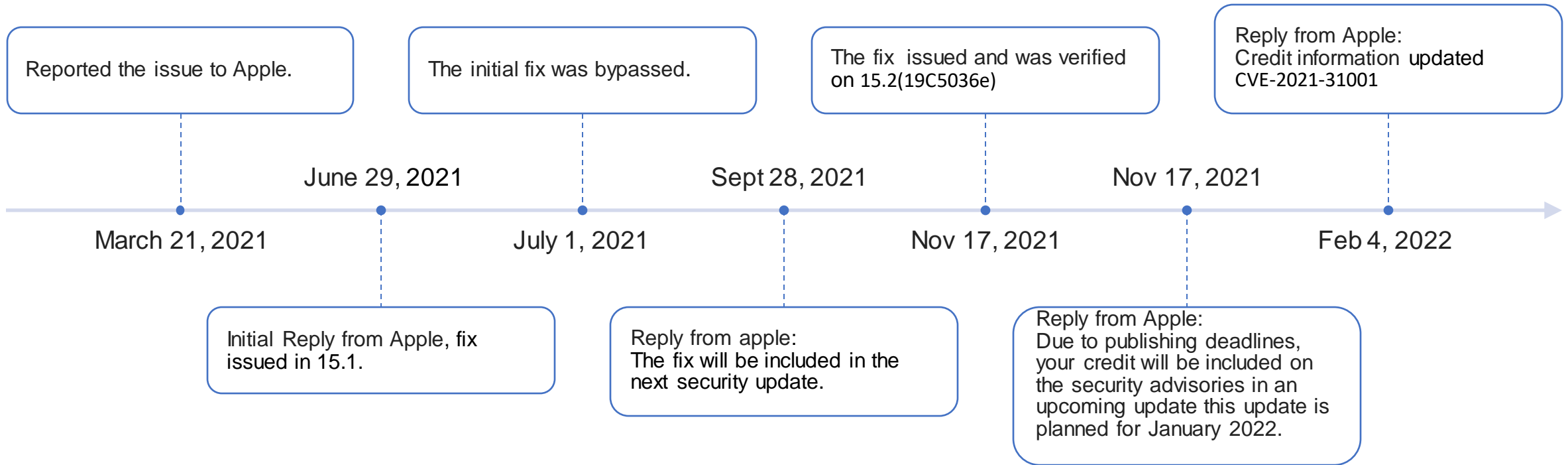
Issue Mitigation

- Fix implementation was done on iOS 15.2(19C5036e) and libIPTelephony terminates and destroys the ImsTcpSocket connection after the IPSec Tunnel has been established.

```
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsTcpSocket: Remote end closed connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsTcpSocket: remote end closed connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [default]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: canceling timer ShutdownWait
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: removing myself from transport
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: KeepAlives not enabled for non-TLS connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: InsecureTransport [100.104.36.221:5060]: terminating
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: closing UDP transport
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsSocket 0x0x141dd6980: invalidating socket 39
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsSocket 0x0x14315eb50: invalidating socket 40
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: Connection closed by both sides.
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: KeepAlives not enabled for non-TLS connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: closing connection
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: ImsSocket 0x0x141ddce10: invalidating socket 49
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: destroying ImsTcpSocket 0x0x141ddce10
```

```
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [default]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: timer IdleTimeout fired
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [net]: shutting down socket
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [sip.tport]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: Connection shutdown attempted. Result = Bambi: Success
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [timer]: registering timer TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060.0x143170990.ShutdownWait
Nov 17 02:39:13 w00ts-iPhone CommCenter(libIPTelephony.dylib)[94] <Notice>: [default]: TcpConnection 100.104.36.221:5060 <-> 10.225.50.20:5060: started timer ShutdownWait with duration 1000ms
```

Issue Timeline

Reported the issue to Apple.

The initial fix was bypassed.

The fix issued and was verified on 15.2(19C5036e)

Reply from Apple:
Credit information updated
CVE-2021-31001

June 29, 2021

Sept 28, 2021

Nov 17, 2021

March 21, 2021

July 1, 2021

Nov 17, 2021

Feb 4, 2022

Initial Reply from Apple, fix issued in 15.1.

Reply from apple:
The fix will be included in the next security update.

Reply from Apple:
Due to publishing deadlines, your credit will be included on the security advisories in an upcoming update this update is planned for January 2022.

THANK YOU!

"Great things are done by a series of small things brought together."

Vincent Van Gogh