

What's Wrong With Fast VoLTE Deployments?

We have already published the conditions of VoLTE deployment (**Volte roaming and the security implications**) in many Mobile Network Operators (MNOs) around the world. Now, we will showcase examples of potentially risky misconfigurations.

Due to the legacy of mobile networks, operators often assume their infrastructure is isolated from subscribers, the internet, and the broader external environment – the wild world. Consequently, they may neglect proper segmentation, firewalls, and Access Control Lists (ACLs). This is because their traditional infrastructure is typically hidden away from prying eyes, leading them to deploy VoLTE infrastructure in a manner similar to other telecom subsystems.

However, operators fail to consider that VoLTE infrastructure is accessible to subscribers just like any other IT infrastructure. Through various VoLTE Security Assessments, we have observed a common scenario where **management interfaces and unnecessary services are exposed/accessible to regular subscribers of VoLTE networks.**

```
# Nmap 7.80 scan initiated [redacted] as: /usr/bin/nmap -sT -n -Pn -vvv --[redacted]
# Ports scanned: TCP(1000;1,3-4,6-7,9,13,17,19-26,30,32-33,37,42-43,49,53,70,79-85,88-90,99-100,106,109-111,113,119,125,135,139,143-144,146,161,163,179,199,211-212,222,254-256)
Host: 10.[redacted].1 () Status: Up
Host: 10.[redacted].1 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].129 () Status: Up
Host: 10.[redacted].129 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].161 () Status: Up
Host: 10.[redacted].161 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].186 () Status: Up
Host: 10.[redacted].186 () Ports: 5060/open/tcp//sip/// Ignored State: filtered (999)
Host: 10.[redacted].250 () Status: Up
Host: 10.[redacted].250 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].1 () Status: Up
Host: 10.[redacted].1 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].33 () Status: Up
Host: 10.[redacted].33 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].97 () Status: Up
Host: 10.[redacted].97 () Ports: 21/open/tcp//ftp///, 22/open/tcp//ssh///
Host: 10.[redacted].5 () Status: Up
Host: 10.[redacted].5 () Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6006/open/tcp//X11:6///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//ht
Host: 10.[redacted].35 () Status: Up
Host: 10.[redacted].35 () Ports: 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 8000/open/tcp//http-alt///
Host: 10.[redacted].37 () Status: Up
Host: 10.[redacted].37 () Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 8000/open/tcp//http-alt///, 8001/open/tcp//vcom-tunnel///
Host: 10.[redacted].41 () Status: Up
Host: 10.[redacted].41 () Ports: 6000/open/tcp//X11///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//http-alt///, 8099/open/tcp//unknown///
Host: 10.[redacted].61 () Status: Up
Host: 10.[redacted].61 () Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6006/open/tcp//X11:6///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//ht
Host: 10.[redacted].63 () Status: Up
Host: 10.[redacted].63 () Ports: 22/open/tcp//ssh///, 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//http-alt///, 8001/open/tcp//
Host: 10.[redacted].69 () Status: Up
Host: 10.[redacted].69 () Ports: 6000/open/tcp//X11///, 6001/open/tcp//X11:1///, 6100/open/tcp//synchronet-db///, 8000/open/tcp//http-alt///
# Nmap done at [redacted]
```

As a telecom security company, we have conducted scans of VoLTE infrastructure, revealing **numerous nodes with open SSH, FTP, X11, and web-management interfaces, all accessible to regular subscribers.**

```
#####
# ATTENTION: AUTHORIZED PERSONAL ONLY. DISCONNECT IMMEDIATELY #
#####

User Authentication
Enter password:
User Authentication
Enter password:

sguser@ims:~$ ssh admin@10.[redacted].129

#####
# ATTENTION: AUTHORIZED PERSONAL ONLY. DISCONNECT IMMEDIATELY #
#####

User Authentication
Enter password:
The user has been locked and you cannot log on it.User Authentication
Enter password:
```

This improper segmentation of the VoLTE network is immediately apparent, but delving deeper reveals issues such as **improper P-CSCF configuration and a lack of encryption.** Consequently, subscribers may be able to view the identities of internal nodes during the registration process.

```

32 416.6601  192.168.1.100      192.168.1.100      SIP      1230      Request: SUBSCRIBE sip:10.205.32.183
33 416.0455  192.168.1.100      192.168.1.100      SIP      1110      Status: 200 OK
35 417.0052  192.168.1.100      192.168.1.100      SIP/XML   990       Request: NOTIFY sip:10.205.32.183

Frame 33: 1128 bytes on wire (9044 bits), 1128 bytes captured (9044 bits) on interface emu0c3b0f270e04, 0.0
Ethernet II, Src: HuaweiE_M7600S (08:0d:fa:9b:9b:a3), Dst: 00:50:07:27:0a:04 (0c:5b:07:27:0a:04)
Internet Protocol Version 4, Src: 192.168.32.183, Dst: 192.168.1.100
Encapsulating Security Payload
User Datagram Protocol, Src Port: 9990, Dst Port: 7200
Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 OK
  Message Header
    Via: SIP/2.0/UDP 10.144.195.183:7200;branch=z9hG4bK-Qp3P2c1kvZ946GIa9KzE8YSbt4w0qU;rport=6200;transport=UDP
    Record-Route: <sip:10.205.32.183:9990;lr;Hpt=mw_1c8_64e72b96_1686af34_ex_8fa2_116;CtxId=3;TRC=ffffffff-ffffffff>
    Call-ID: xdgZnFBF@192.168.1.100
    [Generated Call-ID: xdgZnFBF@192.168.1.100]
    From: <sip:10.205.32.183@ims.mnc001.mcc000.3gppnetwork.org>;tag=xdgZnFBF
    To: <sip:192.168.1.100@ims.mnc001.mcc000.3gppnetwork.org>;tag=dfp5hc2d
    CSeq: 1 SUBSCRIBE
    [Truncated]Contact: <sip:username_mw_1c8_64e72b96_1686af34_k0t1HdtmXh314ca1pge2roJ7Mn75p9Fh+mYpWJdy6UBPZdK0eYeNnfXe6u4JEJJCrvLUXj+m00qhqUs8t010g3aP18rkG5BnaBHYHtWpQJq1wm>
    Expires: 60000
    P-Asserted-Identity: <sip:192.168.1.100-scscf01.ims.mnc001.mcc000.3gppnetwork.org>
    Content-Length: 0
  
```

It's not just the internal infrastructure that's at risk; **there's also the potential exposure of other subscribers' information.** For instance, during a call, it's possible to obtain details such as the calling subscriber's phone model and even their firmware version.

```

3 0.103428398  192.168.1.100      192.168.1.100      SIP      390 Status: 100 Trying |
4 1.791051046  192.168.1.100      192.168.1.100      SIP/SDP   1406 Status: 183 Session Progress |

Frame 4: 1406 bytes on wire (11248 bits), 1406 bytes captured (11248 bits) on interface emu0c3b0f270e04, 0.0
Ethernet II, Src: HuaweiE_M7600S (08:0d:fa:9b:9b:a3), Dst: 00:50:07:27:0a:04 (0c:5b:07:27:0a:04)
Internet Protocol Version 4, Src: 192.168.32.183, Dst: 192.168.1.100
Encapsulating Security Payload
User Datagram Protocol, Src Port: 9990, Dst Port: 7200
Session Initiation Protocol (183)
  Status-Line: SIP/2.0 183 Session Progress
  Message Header
    Via: SIP/2.0/UDP 192.168.1.100:7200;branch=z9hG4bK-ZLqLmZA77nrb1TSQdx0go87WHBmCF70L
    Record-Route: <sip:192.168.1.100:9990;lr;Hpt=mw_276_6504196c_18079c9d_ex_9032_116;CtxId=3;TRC=ffffffff-ffffffff;X-HmB2bUaCookie=19477>
    Call-ID: jbcvxnIe@192.168.1.100
    [Generated Call-ID: jbcvxnIe@192.168.1.100]
    From: <sip:192.168.1.100@ims.mnc001.mcc000.3gppnetwork.org>;tag=jbcvxnIe
    To: <tel:192.168.1.100>;tag=t0a426t4;phone-context=ims.mnc001.mcc000.3gppnetwork.org
    CSeq: 1 INVITE
    Allow: INVITE,ACK,CANCEL,BYE,UPDATE,PRACK,MESSAGE,REFER,NOTIFY,INFO,OPTIONS
    Contact: <sip:192.168.1.100:9990;Hpt=mw_276_6504196c_18079c9d_ex_9032_116;CtxId=3;TRC=ffffffff-ffffffff>;+g.3gpp.icsl-ref="urn:k3Aurn-7k3A3gpp-service.ims.icsl.mmt
    Require: 100rel
    Server: Xicomi_22081212UG_Qualcomm_V13.0.11.0_SLFEXM_Android12;
    CSeq: 1
    P-Early-Media: gated
    P-Asserted-Service-Info: vrbt=00
    Feature-Caps: *;+g.3gpp.srvcc
    Recv-Info: g.3gpp.state-and-event-info
    Content-Length: 350
    Content-Type: application/sdp
  
```

Additionally, the location of the calling subscriber using Cell-ID information.




```

59 10:51:05,967669 2000:4000:2000::2:6060 -> 2000:4000:2000::2:6301 SIP/SDP 812 Status: 183 Session Progr
60 10:51:06,011233 2000:4000:2000::2:6060 -> 2000:4000:2000::2:6301 TCP 116 6060 -> 6301 [ACK] Seq=908
61 10:51:06,011252 2000:4000:2000::2:6060 -> 2000:4000:2000::2:6301 TCP 116 6060 -> 6301 [ACK] Seq=908
62 10:51:06,343276 2000:4000:2000::2:6060 -> 2000:4000:2000::2:6301 SIP 1004 Request: PRACK sip:

<
> Frame 62: 1004 bytes on wire (8032 bits), 1004 bytes captured (8032 bits)
> Linux cooked capture v2
> Internet Protocol Version 6, Src: 2000:4000:2000::2:6060, Dst: 2000:4000:2000::2:6301
> Encapsulating Security Payload
> Transmission Control Protocol, Src Port: 6060, Dst Port: 6301, Seq: 9083, Ack: 5818, Len: 887
> Session Initiation Protocol (PRACK)
  > Request-Line: PRACK sip:[redacted]:6300 SIP/2.0
  > Message Header
    > Via: SIP/2.0/TCP [redacted]:6060;oc-algo="loss";oc;branch=z9hG4bKnavodi-0-264-1e1-1-2000000-b15100
    Max-Forwards: 68
    > From: sip:[redacted]@ims.mnc[redacted].mcc[redacted].3gppnetwork.org;tag=mavodi-__~rwusztvxxw__0-10d-d4-5-ffffff-149b
    > To: <tel:[redacted];phone-context=ims.mnc[redacted].mcc[redacted].3gppnetwork.org>;tag=6ea49803
    Call-ID: FA163EF68208-13ca-137c6700-d93110-61c97361-da2cc
    [Generated Call-ID: FA163EF68208-13ca-137c6700-d93110-61c97361-da2cc]
    > CSeq: 2 PRACK
    > Rack: 1 1 INVITE
    Allow: ACK,BYE,CANCEL,INFO,INVITE,MESSAGE,NOTIFY,OPTIONS,PRACK,REFER,UPDATE
    User-Agent: [redacted]
  > P-Access-Network-Info: 3GPP-E-UTRAN-FDD;local-time-zone="[redacted]";utran-cell-id-3gpp=[redacted]
    access-type: 3GPP-E-UTRAN-FDD
    local-time-zone=[redacted]
    utran-cell-id-3gpp: [redacted]17097140e
  Content-Length: 0
  
```

This list of significant issues doesn't demand a sophisticated hacker; one can acquire this information by simply conducting a **basic nmap-scan and passively analyzing the flow of packets from the subscriber's side.**

In conclusion, the prevailing mindset among many Mobile Network Operators (MNOs) remains rooted in the belief of isolation. This perspective contributes to the persistence of elementary IT-related security issues within VoLTE networks.

About SecurityGen

SecurityGen is a global company focused on telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure safe and robust network operations. Our extensive product and service portfolio provides complete protection against existing and advanced telecom security threats.

Connect With Us

- ✉ Email: contact@secgen.com
- 🌐 Website: www.secgen.com

UK | Italy | Czech Republic | Brazil | India | South Korea | Japan | Malaysia | UAE | Egypt | Lebanon