O2 Flaw Leaked Customer Geolocation Data to Any Caller - Security Spotlight

UK telecom giant O2 has resolved a critical privacy vulnerability that exposed customers' real-time geolocation and device identifiers to anyone who simply initiated a VoLTE phone call. The flaw, present for at least several months, allowed any threat actor to extract precise location data and sensitive network identifiers without any specialized equipment or prior access.

The issue was uncovered by security researcher Daniel Williams during routine network testing. Using a rooted Google Pixel 8 and the Network Signal Guru (NSG) app, Williams initiated a VoLTE call to another O2 customer. He was surprised to find that O2's Session Initiation Protocol (SIP) responses—used to establish internet-based phone calls—were significantly more verbose than those seen on other networks.

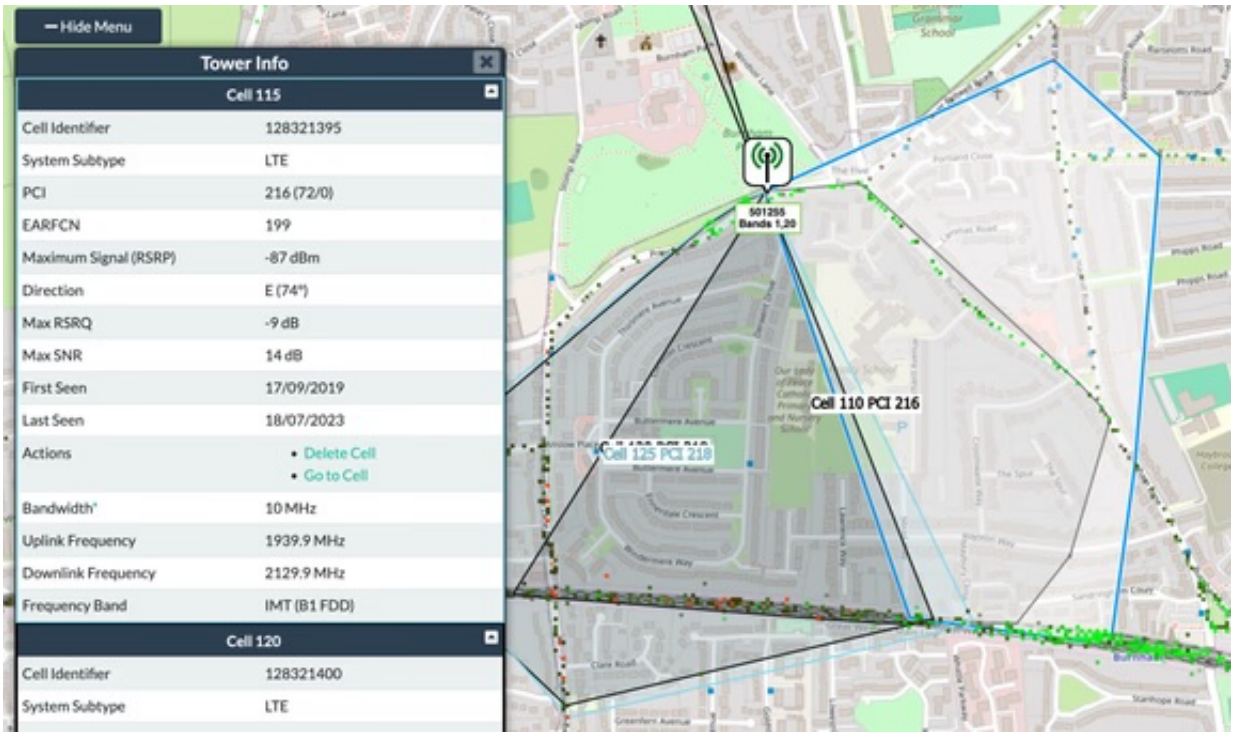
> *"The SIP responses were unlike anything I had seen before on other networks,"*
> — ***Daniel Williams, Security Researcher***

These SIP responses included detailed metadata from O2's core network. Among the exposed data were five particularly alarming SIP headers:

- **Caller and recipient IMSI (International Mobile Subscriber Identity) codes**
- **Caller and recipient IMEI (International Mobile Equipment Identity) numbers**
- **Network identifiers including Location Area Code (LAC) and Cell ID of the recipient**

The Cell ID in particular allowed the attacker to determine the specific

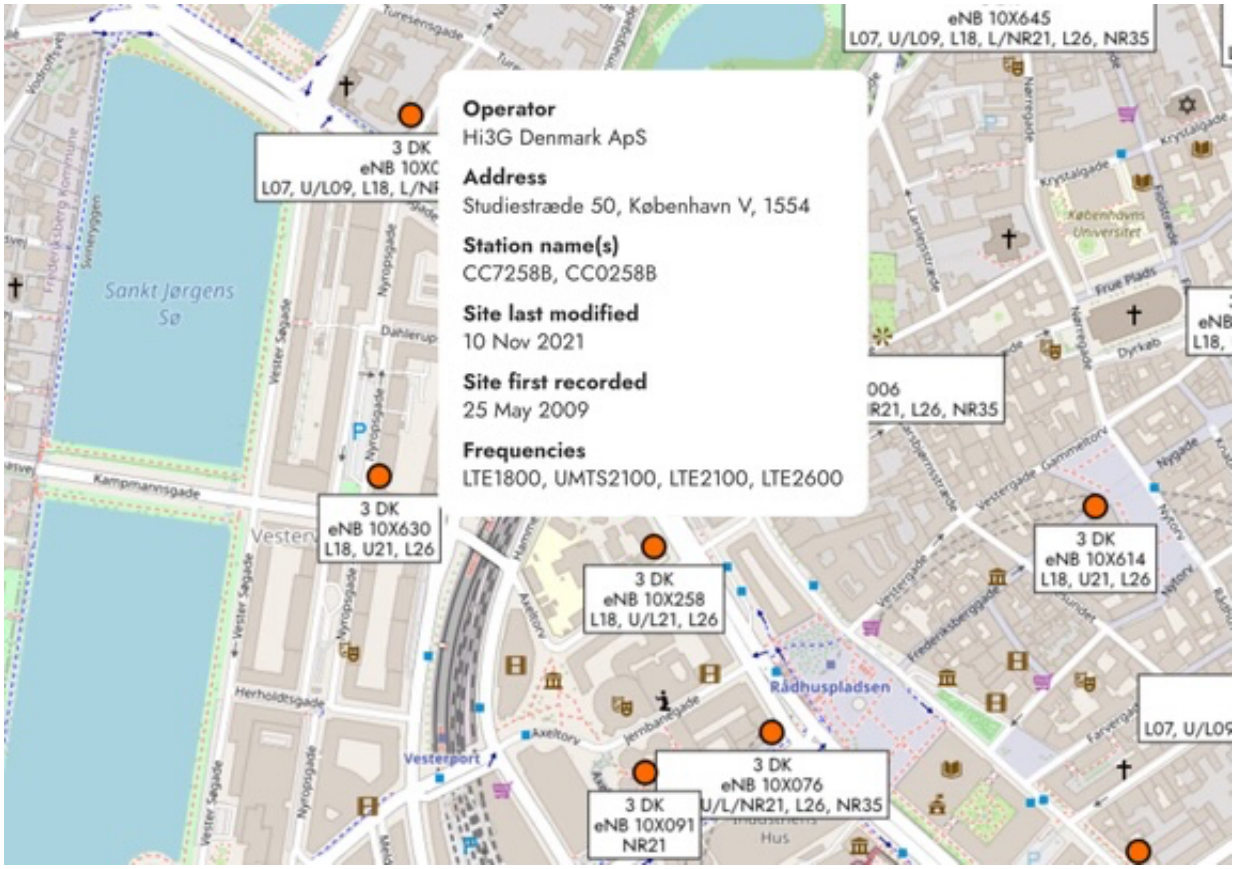
mobile tower the recipient was connected to at the time of the call. In dense urban areas, such towers often serve areas as small as 100 square meters, allowing highly accurate real-time geolocation. Using publicly available databases like CellMapper, Williams was able to map these identifiers to physical locations with high precision.



> *"In a city, this becomes an extremely accurate measure of location."*
> *— Daniel Williams*

The vulnerability also affected users who were roaming internationally. In one demonstration, Williams was able to pinpoint the recipient's location in downtown Copenhagen, Denmark, despite them being thousands of miles from the UK.

> *"The attack worked perfectly with me being able to pinpoint them to the city centre of Copenhagen, Denmark."*
> *— Daniel Williams*



He emphasized that the attack required no malware, phishing, or elevated permissions—just a basic VoLTE-compatible smartphone making a standard call.

Williams first attempted to notify O2 on March 26 and again on March 27. He received no acknowledgment, prompting him to publicly disclose the vulnerability on May 17. Two days later, O2 contacted Williams, confirming the issue had been resolved. Williams verified the fix and confirmed that SIP responses no longer contained the leaked data.

> *"I'm extremely disappointed as an O2 customer to see a lack of any escalation route to report this kind of potential vectors for attack."*
> *— Daniel Williams*

While O2 has since remediated the flaw, the case highlights systemic issues in telecom security and disclosure procedures.