CEL-3 · Mobile Threat Catalogue

Archived: 2026-04-06 00:47:10 UTC

Mobile Threat Catalogue

Downgrade Attacks via Rogue Base station

Contribute

Threat Category: Cellular Air Interface

ID: CEL-3

Threat Description: A rogue base station could force a device to temporarily downgrade its communication standard to a previous cellular network generation. This can make the communication more susceptible to security and privacy issues.

Threat Origin

3G Security: Security Threats and Requirements (Release 4) [1]

LTE Architecture Overview and Security Analysis (Draft NISTIR 8017) [2]

LTE Security and Protocol Exploits [3]

Exploit Examples

Researchers exploit cellular tech flaws to intercept phone calls [4]

Every LTE call, text, can be intercepted, blacked out, hacker finds [5]

CVE Examples

Not Applicable

Possible Countermeasures

Original Equipment Manufacturer

Ensure baseband firmware prevents the use of insecure cellular encryption algorithms

Mobile Network Operator

Use of application layer encryption technologies

References

1. 3G Security; Security Threats and Requirements (Release 4), 3GPP TS 21.133 V4.0.0, 3rd Generation Partnership Project, 2003; www.3gpp.org/ftp/tsg_sa/wg3_security/_specs/Old_Vsns/21133-400.pdf [Accessed 8/23/2016] ↩

2. J. Cichonski, J.M. Franklin, and M. Bartock, NIST Special Publication 800-187: Guide to LTE Security, National Institute of Standards and Technology, 2017; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-187.pdf [Accessed 3/29/2022] ↩

3. R.P. Jover, LTE Security and Protocol Exploits, presented at ShmooCon, 3 Jan. 2016; www.ee.columbia.edu/~roger/ShmooCon_talk_final_01162016.pdf [accessed 8/23/2016] ↩

4. J. Vijayan, “Researchers Exploit Cellular Tech Flaws to Intercept Phone Calls”, ComputerWorld, 1 Aug. 2013; http://www.computerworld.com/article/2484538/cybercrime-hacking/researchers-exploit-cellular-tech-flaws-to-intercept-phone-calls.html [accessed 8/23/2016] ↩

5. D. Pauli, “Every LTE call, text, can be intercepted, blacked out, hacker finds”, The Register, 23 Oct 2016; http://www.theregister.co.uk/2016/10/23/every_lte_call_text_can_be_intercepted_blacked_out_hacker_finds/ [accessed 10/26/2016] ↩
