5G NETWORK VULNERABILITIES AND EXPLOITATION

THIS NEWSLETTER IS A PRODUCT OF THE OUSW FUTUREG PROGRAMS OFFICE IN PARTNERSHIP WITH IDAHO NATIONAL LABORATORY

OUSW Newsletter

SUMMARY

This report summarizes information on vulnerabilities associated with the 5G network that have been or could have been employed or leveraged by an untrusted network operator for exploitation. The report supports the Office of the Under Secretary of War for Research and Engineering (OUSW R&E) FutureG Advanced Component Development and Prototypes Program. The information in this report is based on open-source material published or made available between Aug. 1, 2024, and Sept. 30, 2025. It also contains the potential attack areas that the Idaho National Lab (INL) 5G security research and assessment team has identified from its security analysis.

NOVEL 5G ATTACK BYPASSES NEED FOR MALICIOUS BASE STATION

Singapore University of Technology and Design researchers discovered a way to compromise 5G networks without using a malicious base station. The researchers used and released a framework they refer to as Sni5Gect[1]. The framework can be used to sniff messages and perform message injections in 5G communications. New Radio is a radio technology, powering 5G networks, that is targeted in the attack. The researchers indicated previous 5G attacks involved the use of a malicious base station, requiring the victim connects, severely limiting the practicality of an attack[2].

Key security concerns, putting public safety, national security, and privacy at risk, include:

Device compromise and denial-of-service[3, 4]

- **Crashing devices:** An attacker can inject malformed signaling messages during the device's network connection process. This can overwhelm the mobile modem's protocol state machine, causing the phone or connected device to crash and reboot.
- **Denial of service:** The ability to crash devices can lead to denial-of-service attacks that disrupt critical communications for individuals, businesses, and essential infrastructure.

Degradation to insecure 4G networks[5,6]

- **Forced downgrade:** The attack forces a device to fall back from the more secure 5G network to the less secure 4G network. This exposes devices to a broader range of known, existing vulnerabilities that affect 4G networks.
- **Enables surveillance:** By downgrading a device to 4G, an attacker can leverage legacy vulnerabilities to perform surveillance activities like tracking a user's location over time.

Difficulty of detection[7,8]

- **Stealthy operation:** The Sni5Gect attack operates by manipulating signaling messages rather than setting up a conspicuous rogue base station. This makes it stealthier and increases the risk of delayed detection by network operators.
- **Avoid authentication:** The attack exploits the unencrypted portion of the connection process that occurs before 5G authentication and encryption kick in. As a result, the threat model does not require knowledge of a user's credentials to sniff or inject messages.

Ease of execution[9,10]

- **Off-the-shelf hardware:** Unlike traditional attacks requiring expensive and complex equipment, Sni5Gect can be performed using a laptop and a software defined radio, a readily available piece of equipment.

22-50105

- **Open-source tool:** The framework for the Sni5Gect attack has been released as open source by its discoverers. While intended for security research, this also means the tools are available to malicious actors, lowering the barrier to entry.

Potential for sophisticated attacks[11]

- **Sophisticated actors:** Given its technical complexity, the attack may be leveraged by sophisticated threat actors, such as state-sponsored groups, to cause widespread disruption to telecommunications infrastructure.
- **Steppingstone to more complex attacks:** Researchers warn that Sni5Gect is a fundamental building block that can be combined with legacy attacks to enable more complex and dangerous attacks.

Impact on critical sectors[12]

- **Targeted sectors:** Industries that rely on stable mobile communications, such as telecommunications companies, public infrastructure, and government communications, are particularly vulnerable.
- **Erosion of trust:** The attack's ability to disrupt service and compromise security erodes public and corporate trust in the reliability of 5G networks.

On Aug. 26, Sni5Gect's first version was released, supporting time division duplex (TDD) bands with a 30 kHz subcarrier spacing. The following configurations were tested:[13]

- Frequency bands: n78 and n41 (TDD)
- Frequency: 3427.5 MHz and 2550.15 MHz
- Subcarrier spacing: 30 kHz
- Bandwidth: 20–50 MHz
- MIMO configuration: Single-input single-output
- Distance: 0 to 20 meters (with amplifier)

Additional capabilities were added and tested in a second version released Sept. 17, including:[14]

- Dual-channel frequency division duplexing (FDD) support: Receive and process IQ samples from two channels simultaneously using software-defined radios with dual RX chains.
- Unified codebase for 15 kHz and 30 kHz subcarrier spacing without recompilation.
- Expanded testing with the following setups:
    - Frequency bands:
        - TDD: n78 and n41
        - FDD: n3
    - Frequency: 3427.5 MHz, 2550.15 MHz, and 1865.0 MHz
    - Subcarrier spacing: 30 kHz and 15 KHz

The notable difference of the Sni5Gect attack is the attacker is in range of the victim and is able to intercept unencrypted messages exchanged between the base station and the targeted user's phone. The connection is targeted prior to authentication so the traffic is not protected, which allows the attacker to access without requiring the device's credentials. The attacker simply waits for the targeted phone to lose connection, then reinitiates the device. The following figure shows an illustration of the Sni5Gect attack.

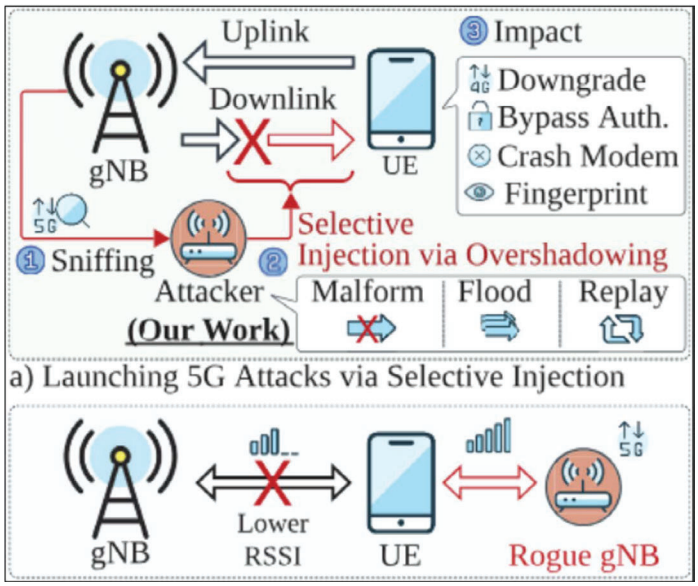

Figure 1: Illustration of Sni5Gect attack[15]

Reconnecting to the network is a common practice for the devices, this can include when the user disables airplane mode after a flight, when passing through a tunnel or underground parking garage, or when riding an elevator.[16,17] If the attacker can initialize an attack prior to the connection being secured, they can intercept unencrypted messages and inject malicious payloads. The attacker can then disable the modem associated with the victim's device, fingerprint, track the targeted device, and downgrade the connection to 4G. Once downgraded to 4G, the attacker can exploit known vulnerabilities within that network. According to the researchers, Sni5Gect attack has been tested against five smartphones, including OnePlus Nord CE 2, Samsung Galaxy S22, Google Pixel 7, and Huawei P40 Pro.[18]

The tests were 80% accurate to the uplink and downlink sniffing, and injected message success was 70-90% from a distance of up to 65 feet (20 meters). One of the

researchers, Yee Ching Tok, explained "Compared to prior state-of-the-art works, the Sni5Gect framework does not require rogue gNodeB (gNB) stations when executing over-the-air sniffing and stateful injections. The absence of a rogue gNB is significant as it reduces setup complexities while increasing stealth."[19]

"GSMA, the organization that represents the interests of mobile network operators, has acknowledged the findings and assigned the attack the identifier CVD-2024-0096 (CVD rather than CVE identifiers are assigned to security issues affecting the mobile industry)."[20]

MITIGATION SUGGESTIONS FOR SNI5GECT ATTACKS:

Mitigating a Sni5Gect attack might require a multi layered approach involving network operators, device manufacturers, and individual users. Since there is no single solution to completely prevent this attack, a combination of methods may be necessary to mitigate an attack.[21, 22]

Suggestions for mobile network operators and vendors:[23, 24]

- **Deploy firmware and software updates:** Operators and equipment vendors must deploy patches to fix vulnerabilities in the 5G control-plane signaling protocols. This is a critical first step to address the specific flaws exploited by Sni5Gect.
- **Enhance authentication protocols:** Stricter authentication mechanisms and session renegotiation protocols can make it more difficult for attackers to manipulate network control messages.
- **Implement advanced anomaly detection:** Network intrusion detection systems should be configured to monitor irregular signaling patterns and unexpected connection renegotiations. Machine learning-based anomaly detection can help identify early indicators of an attack.
- **Use network slicing and isolation:** For private and critical networks, such as military or industrial applications, utilize 5G network slicing to isolate critical communications. This prevents an attack on one network slice from impacting others.
- **Harden firmware and message handling:** Chipset vendors should harden baseband firmware and sanitize pre-authentication message handling to prevent manipulation of messages during the critical connection phase.
- **Collaborate and share threat intelligence:** Communication authorities, vendors, and cybersecurity firms should collaborate to standardize mitigation efforts and share threat intelligence to quickly address new vulnerabilities.
- **Improve 5G standards:** In the medium term, standards bodies like 3GPP and GSMA should improve 5G signaling standards to close inherent protocol weaknesses, potentially by securing or reducing the unprotected pre-authentication window.

Suggestions for individual users:[25, 26]

- **Keep your device and OS updated:** Regularly install software and modem firmware updates from your device's manufacturer and mobile carrier. These updates often contain critical security patches that address known vulnerabilities.
- **Consider disabling older network generations:** If your device allows it, disable older network protocols like 2G and 3G. Sni5Gect is often used to force a device to downgrade from 5G to 4G, so disabling even older, more vulnerable standards can reduce risk. However, this comes with the trade-off of potentially losing service in areas without good 4G or 5G coverage.
- **Turn on airplane mode during sensitive conversations:** For high-security situations, like a confidential meeting, the safest approach is to enable airplane mode or leave your device behind. This completely prevents network interception.
- **Monitor for suspicious activity:** Pay attention to your phone's behavior. An attack that causes repeated crashes or network downgrades is suspicious and should prompt you to check for software updates.

OVER 100 LTE AND 5G VULNERABILITIES DISCOVERED

According to Hoplon Infosec, a cyber security team, researchers have discovered 119 vulnerabilities associated with LTE and 5G implementations. These vulnerabilities compromise and access the core of the cellular network. The systems tested were found to have multiple flaws that could allow attackers to compromise up to the core cellular network. The figure 2 represents a cellular network and shows how the core interacts with the network.[27]

Key security concerns, putting public safety, national security, and privacy at risk include:[28, 29, 30]

- Communication disruption: Attackers could cause city wide denial of service by crashing network components like the mobility management entity in LTE or access and mobility management function in 5G. Some exploits require only a single, malformed packet from an unauthenticated device, potentially disrupting calls, messages, and data services for an entire area.

- Surveillance: The flaws could allow attackers to monitor the location and connection data of subscribers within a city. Unauthorized access to the core network could also enable monitoring and manipulation of communications for data theft and espionage.
- New attack vectors: Wi-Fi calling can make exploitation more widespread by allowing remote attacks over the internet. Accessible 5G base stations and home femtocells also create potential entry points for adversaries.
- Supply chain risks: The complex supply chain for 5G components increases the risk of compromised hardware and software. Using untrusted vendors or integrating with older, vulnerable 4G infrastructure can also expose the network to risks.

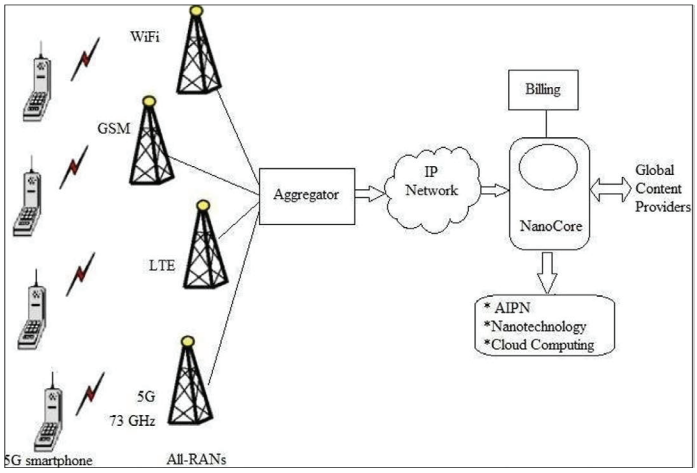

Figure 2: Cellular network[31]

Every vulnerability could result in a denial of service that is persistent in nature, possibly affecting an entire city. The exploitation of these vulnerabilities has the potential to disable critical components in the network such as mobility management entity in LTE, or the access and mobility management function in 5G networks.[32]

The compromises can be imitated by a single packet that carries malicious data over the network with no SIM card or authentication required to successfully execute the attack. The network could experience this compromise on a persistent basis until the operators notice, and an appropriate patch is installed.[33]

According to the researchers, other effects of the vulnerabilities could include buffer overflows and memory corruption. Once inside the network, the attackers may have the ability to:[34]

- Monitor location and connection data for all subscribers within a city[35]
- Conduct targeted attacks on specific individuals[36]
- Compromise critical network components like the home subscriber service or unified data management, potentially extending disruptions nationwide [37]

The researchers concluded there are two primary threat models, unauthorized device exploits and base station exploits.

- Unauthorized device exploits can be utilized with any mobile device that can send malformed packets over the network and can be launched remotely depending on the calling service[38]
- Base station exploits can execute misconfigurations or leaked IPsec keys to access the core[39]

VULNERABILITY FOUND: A SINGLE PACKET CAN PARALYZE SMARTPHONES

Korea Advanced Institute of Science and Technology (KAIST) researchers discovered vulnerabilities in the lower layers of smartphone communication modems and demonstrated the need to standardize mobile communication modem security testing. The discovered vulnerabilities could incapacitate smartphone communications using a single manipulated wireless packet (a data transmission unit in a network). These vulnerabilities score high on severity, potentially leading to remote code execution. The team used and developed a testing framework called lower layer fuzz (LLFuzz) to

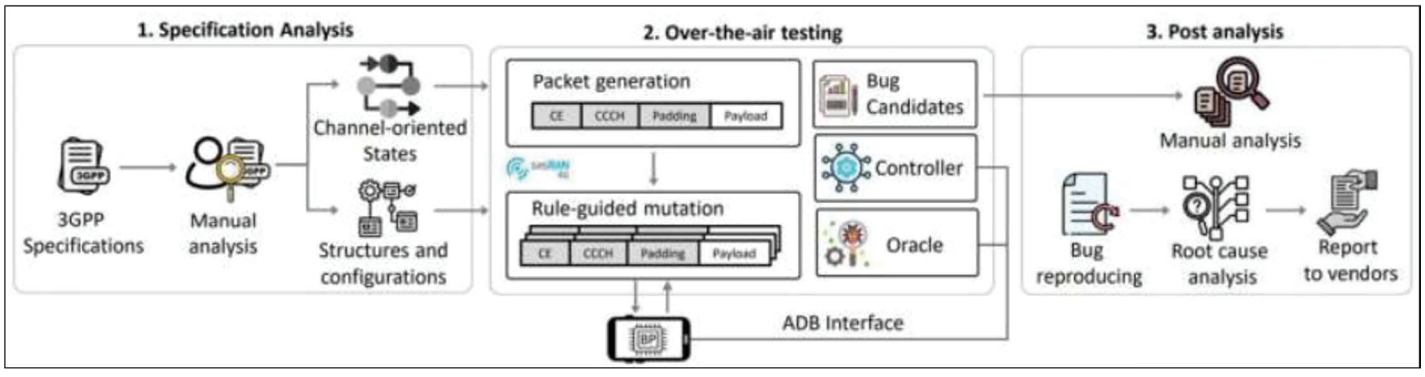

Figure 3: KAIST testing and analysis

complete the testing successfully.[40] The following figure represents pre analysis, testing, and post analysis flow.

LLFuzz used analysis framework to understand the lower layer state transitions and error handling logic of the modem, detecting security vulnerabilities. The framework precisely extracted vulnerabilities caused by implementation errors by comparing and analyzing 3GPP (mobile broadband standard) with actual device responses. Experiments were conducted on 15 commercial smartphones from global manufacturers, including Apple, Samsung Electronics, Google, and Xiaomi, and discovered a total of 11 vulnerabilities. Seven of the discovered vulnerabilities were assigned CVE numbers, and manufacturers created security patches for those vulnerabilities. The remaining four have not yet been publicly disclosed as of July 2025.[41]

What makes this research unique is previous security research primarily focused on higher layers of mobile communication, such as network access stratum and radio resource control, this research focused on analyzing the error handling logic of mobile communication's lower layers, which manufacturers could neglect. These vulnerabilities occurred in the lower layers of the communication modem—Radio Link Control (RLC), Medium Access Control (MAC), Packet Data Convergence Protocol (PDCP), and Physical layer (PHY). Due to the structural characteristics, encryption or authentication are not applied and could cause operational errors by injecting external signals.[42]

"The vulnerabilities were found in the modem chip, a core component of smartphones responsible for calls, texts, and data communication, making it a very important component.

- Qualcomm: Affects over 90 chipsets, including CVE-2025-21477, CVE-2024-23385
- MediaTek: Affects over 80 chipsets, including CVE-2024-20076, CVE-2024-20077, CVE-2025-20659
- Samsung: CVE-2025-26780 (targets the latest chipsets like Exynos 2400, 5400)
- Apple: CVE-2024-27870 (shares the same vulnerability as Qualcomm CVE)"[43]

The chips in question are in low-and high-end smart phones. The associated low layer vulnerabilities were found in just two weeks by the team, and it is likely more vulnerabilities exist in this layer.

Professor Yongdae Kim explained, "The lower layers of smartphone communication modems are not subject to encryption or authentication, creating a structural risk where devices can accept arbitrary signals from external sources. This research demonstrates the necessity of standardizing mobile communication modem security testing for smartphones and other IoT devices." [44]

SOURCES

1 Sni5Gect | https://asset-group.github.io/Sni5Gect-5GNR-sniffing-and-exploitation/#/ | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings

2 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

3 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

4 [RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

5 [RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

6 [Hacker News | "New Sni5Gect Attack Crashes Phones and Downgrades 5G to 4G without Rogue Base Station" | https://thehackernews.com/2025/08/new-sni5gect-attack-crashes-phones-and.html | 26 August 2025 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

7 [RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

8 [Hacker News | "New Sni5Gect Attack Crashes Phones and Downgrades 5G to 4G without Rogue Base Station" | https://thehackernews.com/2025/08/new-sni5gect-attack-crashes-phones-and.html | 26 August 2025 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

9 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

10 [Risky Business News | "Risky Bulletin: Academics Pull Off Novel 5G Attack" | https://news.risky.biz/risky-bulletin-academics-pull-off-novel-5g-attack/# | 17 August 2025 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

11 [RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

12 [RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

13 [Sni5Gect | https://asset-group.github.io/Sni5Gect-5GNR-sniffing-and-exploitation/#/ | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

14 [Sni5Gect | https://asset-group.github.io/Sni5Gect-5GNR-sniffing-and-exploitation/#/ | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

15 [Risky Business News | Catalin Cimpanu | "Risky Bulletin: Academics pull off novel 5G attack" | https://news.risky.biz/risky-bulletin-academics-pull-off-novel-5g-attack/ | 17 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

16 [Risky Business News | Catalin Cimpanu | "Risky Bulletin: Academics pull off novel 5G attack" | https://news.risky.biz/risky-bulletin-academics-pull-off-novel-5g-attack/ | 17 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

17 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

18 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

19 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

20 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

21 [RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

22 [SecurityWeek | "Novel 5G Attack Bypasses Need for Malicious Base Station" | https://www.securityweek.com/novel-5g-attack-bypasses-need-for-malicious-base-station/ | 18 August 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

23 [RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]'

24 [Joanna Śliwa and Marek Suchański | "Security Threats and Countermeasures in Military 5G Systems" | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9924818 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

25 RESCANA | "Sni5Gect Attack Exposes 5G Signaling Flaws in SX-5G Systems, Crashing Phones and Forcing 4G Downgrades" | https://www.rescana.com/post/sni5gect-attack-exposes-5g-signaling-flaws-in-sx-5g-systems-crashing-phones-and-forcing-4g-downgrad# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]'

26 [Joanna Śliwa and Marek Suchański | "Security Threats and Countermeasures in Military 5G Systems" | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9924818 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]'

27 [Hoplon | "Discover 100+ LTE & 5G Vulnerabilities Threatening Security" | https://hoploninfosec.com/discover-100-lte-5g-vulnerabilities/ | Accessed on 29 August 2025 | The source is publicly available information and does not contain classification markings]

28 [Hoplon | "Discover 100+ LTE & 5G Vulnerabilities Threatening Security" | https://hoploninfosec.com/discover-100-lte-5g-vulnerabilities/ | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

29 [Anoushka Das | "RANsacked: Over 100 Security Flaws Found in LTE and 5G Network Implementations" | https://www.linkedin.com/pulse/ransacked-over-100-security-flaws-found-lte-5g-network-anoushka-das-9asle# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

30 [R3 | "5G Security Concerns: Potential Vulnerabilities and Security Measures" | https://www.r3-it.com/blog/5g-security-concerns/# | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

31 [ResearchGate | "5G Network Image" | https://www.researchgate.net/figure/Network-Architecture-for-5G-10-Fig-5-shows-5G-network-architecture-for-mobile-systems_fig3_324941597 | Accessed on 09 September 2025 | The source is publicly available information and does not contain classification markings]

32 [Hoplon | "Discover 100+ LTE & 5G Vulnerabilities Threatening Security" | https://hoploninfosec.com/discover-100-lte-5g-vulnerabilities/ | Accessed on 29 August 2025 | The source is publicly available information and does not contain classification markings]

33 [Hoplon | "Discover 100+ LTE & 5G Vulnerabilities Threatening Security" | https://hoploninfosec.com/discover-100-lte-5g-vulnerabilities/ | Accessed on 29 August 2025 | The source is publicly available information and does not contain classification markings]

34 [Hoplon | "Discover 100+ LTE & 5G Vulnerabilities Threatening Security" | https://hoploninfosec.com/discover-100-lte-5g-vulnerabilities/ | Accessed on 29 August 2025 | The source is publicly available information and does not contain classification markings]

35 [Cyber Security News | Guru Baran | "100+ Vulnerabilities in LTE & 5G Infrastructure Enable Remote Core Compromise" | https://cybersecuritynews.com/100-vulnerabilities-in-lte-5g-implementations/ | January 24, 2025 | Accessed on 10 September 2025 | The source is publicly available information and does not contain classification markings]

36 [Cyber Security News | Guru Baran | "100+ Vulnerabilities in LTE & 5G Infrastructure Enable Remote Core Compromise" | https://cybersecuritynews.com/100-vulnerabilities-in-lte-5g-implementations/ | January 24, 2025 | Accessed on 10 September 2025 | The source is publicly available information and does not contain classification markings]

37 [Cyber Security News | Guru Baran | "100+ Vulnerabilities in LTE & 5G Infrastructure Enable Remote Core Compromise" | https://cybersecuritynews.com/100-vulnerabilities-in-lte-5g-implementations/ | January 24, 2025 | Accessed on 10 September 2025 | The source is publicly available information and does not contain classification markings]

38 [Cyber Security News | Guru Baran | "100+ Vulnerabilities in LTE & 5G Infrastructure Enable Remote Core Compromise" | https://cybersecuritynews.com/100-vulnerabilities-in-lte-5g-implementations/ | January 24, 2025 | Accessed on 10 September 2025 | The source is publicly available information and does not contain classification markings]

39 [Hacker News | "RANsacked: Over 100 Security Flaws Found in LTE and 5G Network Implementations" | https://thehackernews.com/2025/01/ransacked-over-100-security-flaws-found.html | January 24, 2025 | Accessed on 13 October 2025 | The source is publicly available information and does not contain classification markings]

40 [Tech Xplore | The Korea Advanced Institute of Science and Technology | "Vulnerability found: A single packet can paralyze smartphones" | https://techxplore.com/news/2025-07-vulnerability-packet-paralyze-smartphones.html | 29 July 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

41 [Tech Xplore | The Korea Advanced Institute of Science and Technology | "Vulnerability found: A single packet can paralyze smartphones" | https://techxplore.com/news/2025-07-vulnerability-packet-paralyze-smartphones.html | 29 July 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

42 [Tech Xplore | The Korea Advanced Institute of Science and Technology | "Vulnerability found: A single packet can paralyze smartphones" | https://techxplore.com/news/2025-07-vulnerability-packet-paralyze-smartphones.html | 29 July 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

43 [Tech Xplore | The Korea Advanced Institute of Science and Technology | "Vulnerability found: A single packet can paralyze smartphones" | https://techxplore.com/news/2025-07-vulnerability-packet-paralyze-smartphones.html | 29 July 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]

44 [Tech Xplore | The Korea Advanced Institute of Science and Technology | "Vulnerability found: A single packet can paralyze smartphones" | https://techxplore.com/news/2025-07-vulnerability-packet-paralyze-smartphones.html | 29 July 2025 | Accessed on 11 September 2025 | The source is publicly available information and does not contain classification markings]