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 vulnerabilities associated with 5G networks that could be employed or leveraged by an untrusted or rogue network operator (including a compromised operator environment) to impact end users (UEs) on the network. The report is in support 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 relevant in the final quarter of calendar year 2025, supplemented with authoritative vulnerability and security bulletin records used to describe specific issues.

IMS-SERVICE VULNERABILITIES ENABLE NETWORK-TRIGGERED UE IMPACT (MEDIATEK)

MediaTek product security bulletins and public CVE records in 2025 describe flaws in the Android "IMS service" component that can be triggered when a UE connects to an attacker-controlled (rogue) base station. These issues are relevant to an untrusted operator model because a malicious or compromised operator environment can provide the same network-originated inputs that the CVEs describe. In deployments where IMS supports VoLTE, Vo5G and related voice and messaging services, defects in IMS-handling paths are operationally significant because the network is a primary input channel and failures can directly affect user and availability, with potential safety implications if emergency calling is disrupted.

Key security concerns

- Remote denial-of-service (DoS) against the UE: CVE-2025-20678 describes a possible system crash due to incorrect error handling in IMS service, leading to remote DoS when the UE is connected to a rogue base station, with no user interaction required.[1, 2]
- Potential remote privilege escalation path: CVE-2025-20725 describes an out-of-bounds write due to a missing bounds check that could l ead to remote escalation of privilege in a rogue base station threat model (dependent on affected builds and patch status).[3, 4]
- High operational impact surface (voice/IMS plane): Because IMS is tied to voice service continuity and registration workflows, repeated crashes or state corruption can translate into loss of calling, messaging, and emergency communications for impacted users.[5, 6]

Why this matters in an untrusted operator model

- Although public writeups often frame these issues as "rogue base station" threats, the practical distinction for high-risk users is that a visited or roaming network, or a compromised operator environment, can influence similar signaling and protocol conditions at scale. In such scenarios, the network can become an attack surface for triggering device instability, forced re-registration loops, or (in worst cases) privilege escalation conditions. attempts that correlate with specific cells, roaming partners, or configuration changes.[7, 8]
- Clusters of UE reboots/modem resets following IMS registration or voice service negotiation events (where telemetry is available).
- Unusual increases in emergency-calling fallback behavior or voice service unavailability reports in a geographic area.

CLEARED
For Open Publication
15
Jun 18, 2026
Department of War
OFFICE OF PREPUBLICATION AND SECURITY REVIEW

22-50105

Mitigation suggestions (operators, vendors, and users)

- Device/OEMs: Prioritize modem/telephony/IMS updates and ensure patch propagation (device OS + vendor components) addresses IMS service issues (e.g., MediaTek patch IDs referenced in product security bulletins).[9, 10]
- Operators: Treat IMS and voice signaling planes as high-risk surfaces for malformed input; implement robust validation, rate limiting, and anomaly detection around signaling workflows where feasible.[11]
- Programs/assessors: Build regression test cases around network-originated malformed input to telephony/IMS stacks (including pre-call setup, registration, and mobility transitions) and re-run after baseband/telephony updates.
- Enterprise users: Track device patch levels for baseband/telephony components and consider roaming risk controls for high-value travel (e.g., limiting roaming to trusted partners where policy allows).

OVER-THE-AIR BASEBAND/PROTOCOL FUZZING RESEARCH SHOWCASES UE RISK UNDER ROGUE RADIO CONDITIONS (5GHOUL)

A 2025 publication introduces 5Ghoul, a framework designed to systematically discover and replicate security vulnerabilities on 5G user equipment over-the-air using a stateful multi-layer fuzzing strategy. The work emphasizes fine-grained control of packets down to the data link layer and automated construction of protocol state machines to guide fuzzing and improve reproducibility on commercial off-the-shelf (COTS) UEs.[12]

Key security concerns

- Over-the-air exploitability and reproducibility: The paper describes design choices intended to make vulnerabilities reproducible against commercial UEs over the air, aligning with a threat model where the adversary controls radio/network inputs.[13]
- Breadth of impacted devices and vendors: The authors report evaluating 5Ghoul against seven COTS 5G UEs and uncovering multiple previously unknown vulnerabilities, including CVEs assigned for COTS UE issues from major vendors.[14]
- Implementation-level weaknesses in 5G modem stacks: ASSET disclosures characterize 5Ghoul as a family of implementation-level 5G vulnerabilities affecting modem firmware from major chipset vendors, reinforcing that closed-source baseband implementations remain a significant risk area.[15]
- Operator-relevant outcomes: The public tooling and documentation demonstrate that a base-station-side adversary can craft malformed sequences that degrade connectivity, trigger crashes, or keep devices cycling through connection states, producing end-user impact without device-side compromise prerequisites.[16, 17]

Why this matters in an untrusted network operator model

- 5Ghoul is valuable for operator-to-end-user risk discussions because it models a realistic asymmetry: the network controls a large portion of the input surface the UE must parse to attach and operate. A malicious network operator (or a compromised RAN in a legitimate operator) can use that control to target specific users, specific device models, or an entire coverage area. Even when the primary demonstrated outcome is denial-of-service, the operational consequence can be severe (e.g., loss of communications, forced fallback behavior, and increased exposure windows for additional attacks).

Defensive takeaways for operators and assessors

- RAN integrity is a user-safety control: Treat gNB software supply chain, configuration management, and access control as part of UE security because compromised base stations can become active exploitation platforms.[18, 19]
- Test like an adversarial network: Expand security testing coverage with stateful, protocol-aware negative testing (not only spec conformance), particularly around attach/registration, mobility transitions, and lower-layer error handling.[20]
- Detect population-level symptoms: Establish baselines for attach failure rates, abnormal detach/re-attach loops, modem crash reports (where available), and unexpected RAT fallback patterns to detect network-triggered UE instability.

Mitigation suggestions (operators, vendors, and users)

- Vendors: Invest in protocol state-machine validation, robust bounds checking, and continuous fuzzing of baseband stacks using methodologies similar to those described by 5Ghoul.[21]
- Operators/enterprises: Maintain chipset-aware device fleet inventories and enforce patch SLAs for baseband/telephony components; consider risk controls for high-value travel and roaming where hostile network conditions are plausible.[22]

- Programs/assessors: Use public artifacts (e.g., PoC descriptions and test methodology) to derive non-exploitative test cases that validate robustness against malformed radio-side inputs, and verify that mitigations remain effective after vendor updates.[23]

5G CORE SERVICE BASED ARCHITECTURE (SBA) AUTHORIZATION WEAKNESSES CAN EXPAND OPERATOR BLAST RADIUS (CROSS-SERVICE TOKEN)

While many end-user impacts originate in the RAN and baseband, 5G also introduces a cloud-native core with Service-Based Interfaces (SBIs) between network functions. In September 2025, researchers presented FivGeeFuzz, a grammar-based fuzzing framework that derives inputs from 3GPP API specifications and evaluates the security of SBI services. When tested against the free5GC open-source 5G core, the authors reported discovering multiple vulnerabilities leading to runtime crashes, improper error handling, and unauthorized access to resources, including an attack they refer to as "Cross-Service Token".[24]

Key security concerns

- Unauthorized access across network functions: If access tokens or authorization checks are insufficiently scoped or validated, compromise of one network function can enable unauthorized access to resources owned by another function, increasing the likelihood of subscriber-impacting actions.[25]
- Control-plane disruption: The research reports crash and error-handling weaknesses in SBI implementations, which can translate into denial-of-service conditions at the core network layer and indirectly impact end-user service availability.[26]
- Risk amplification through cloud deployment models: Because core network functions are often deployed in shared/cloud environments, insider threats or cloud compromise scenarios can intersect with SBI weaknesses to broaden the operator-side attack surface and subscriber impact.[27]

Operator-to-end-user implications

- In a rogue or compromised network operations scenario, core-network-side weaknesses can produce end-user harm even without exploiting UE baseband code. Examples of subscriber-relevant outcomes include targeted service denial (session establishment failures), unauthorized access to subscriber-related resources, or manipulation of session/policy state that changes how a user's traffic is handled. Even though the cited work evaluates an open-source implementation, the findings are a practical reminder that SBI authorization boundaries are a critical containment control that limits what an attacker can access after a single Network Function (NF) is compromised.[28]

Mitigation suggestions (operators and vendors)

- Treat SBIs as high-risk APIs: Enforce strict authentication (e.g., mutual TLS where applicable) and least-privilege token scoping (audience and scope binding) between network functions; continuously validate token claims at every hop.[29]
- Segment and monitor NF-to-NF traffic: Apply micro-segmentation and egress controls so that a compromised network function cannot arbitrarily reach all other functions; log and alert on unexpected SBI call patterns.[30]
- Continuously test your own core: Integrate fuzzing and negative testing of SBI endpoints into security assurance, including regression testing after upgrades and configuration changes, using approaches similar to those described in the research.[31]

PATCH LAG AND ECOSYSTEM VARIABILITY CAN AMPLIFY NETWORK-ADJACENT RISK (ANDROID / QUALCOMM EXAMPLE)

Patch latency across the mobile ecosystem can meaningfully increase risk for end users exposed to hostile or untrusted network conditions (e.g., roaming, travel, or targeted surveillance). The Android Security Bulletin for August 2025 notes that devices patched to security patch level 2025-08-05 or later address the issues in that bulletin.[32] Public reporting in 2025 also highlighted cases where Qualcomm component vulnerabilities were reported as exploited in limited, targeted attacks, with CISA adding related CVEs to its Known Exploited Vulnerabilities catalog.[33, 34]

Key security concerns

- Uneven patch deployment extends exposure windows: Android's distributed update model means different OEMs and carriers can roll out fixes on different timelines, leaving portions of the user base exposed after a vendor fix exists.[35, 36]
- Documented targeted exploitation: Public sources reported exploitation signals and government alerts for specific Qualcomm vulnerabilities, underscoring that high-value users can be targeted during patch gaps.[37, 38, 39, 40]
- Operational impact on roaming/high-risk populations: For users who must operate on untrusted networks,

patch lag increases the probability that network-adjacent adversaries can chain known device flaws with other access opportunities (e.g., captive portals, malicious content delivery, or exploitation of exposed services).

Mitigation suggestions (programs, operators, enterprises, and users)

- Programs/enterprises: Enforce patch SLAs and minimum-security patch levels for managed mobile fleets; prefer devices/OEMs with a demonstrated ability to deliver timely security updates.[41]
- Operators: Reduce carrier-side deployment delays for critical security patches and maintain mechanisms to prioritize distribution of baseband/telephony-related updates to high-risk populations where possible.
- Users: Keep OS and security updates current, verify the device security patch level, and consider using devices with longer support windows for high-risk roles.[42]

RESEARCH FINDINGS SPOTLIGHT: AI-POWERED CELLULAR PATTERN-OF-LIFE (POL) DISCOVERY

Recent FutureG-sponsored research highlights an adjacent (and often underappreciated) risk to end users operating in untrusted or surveilled environments: even without exploiting device software, cellular signaling metadata can reveal a "pattern of life" (PoL) that enables inference of routines, relationships, and changes in operational tempo. In an experiment led by Chesapeake Technology International (A Parsons Corp. Company) from June to October of 2025, AI/ML analytics were applied to Mobile Network Operator (MNO)-sourced signaling metadata from 38 devices to surface the same behavioral signatures an adversary would prioritize, predictability, clustering, and anomalies.

What PoL analysis revealed

- Anomaly detection surfaced outliers that could indicate handset changes, compromise, or tempo shifts, including IMSI-to-IMEI swaps (10% of devices), abrupt activity spikes/declines (10%), and sudden long-distance location shifts (13%).
- Co-presence analysis mapped group dynamics: 13% of devices repeatedly co-located, forming a "hub" that met frequently (15 meetings). One device (anonymized as device 2154 in the study) repeatedly intersected with the hub, suggesting a potential single point of compromise or surveillance leverage.
- Operational cadence became visible at the group level: the model identified a main activity phase from late July to early August followed by a drop-off consistent with stand-down behavior.
- Participation patterns suggested role/task segmentation: 87% of devices appeared as "one-time transients," consistent with temporary or task-based involvement rather than persistent participation.
- Routine discovery highlighted that a small subset (5%) exhibited highly predictable daily behavior. In one example (device 2155), the device was consistently stationary until 3 PM JST, followed by movement that still followed a discernible loop, illustrating how even partial regularity can be exploited for surveillance and targeting.
- Baseline modeling enabled detection of behavioral shifts, changes in routine that can signal a new mission phase, a changed role, or altered status.

Why this matters in an untrusted environment

The findings reinforce that cellular exposure is not limited to technical exploitation of modems or core networks. Entities with access to signaling metadata (e.g., a malicious or compromised operator environment) or those who can acquire comparable location/association data via RF observation, commercial feeds, or OSINT can derive actionable intelligence about who is co-located with whom, when routines occur, and when behavior deviates from baseline. This expands the operational risk landscape: even "non-exploit" visibility can enable targeting, attribution of organizational relationships, and prediction of future movements.

Defensive takeaways

- Treat signaling metadata as sensitive: PoL can be derived from metadata alone, so storage, sharing, and access controls should be commensurate with mission impact.
- Reduce predictability where feasible: routine regularity and repeated co-location are high-signal indicators for surveillance analytics; introduce variability in schedules and meeting patterns when operationally acceptable.
- Monitor for anomalies as early warning: IMEI/IMSI association changes, abrupt activity shifts, and unusual travel can be used as triggers for review, containment actions, or OPSEC checks.
- Use PoL analytics as a complementary control: integrate behavioral baselining with device patching and network assurance so that both "exploitation" and "observability" risks are managed in parallel.

SOURCES

1 MediaTek | "June 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/June-2025 | 2 June 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

2 National Vulnerability Database (NVD) | "CVE-2025-20678 Detail" | https://nvd.nist.gov/vuln/detail/CVE-2025-20678 | 1 June 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

3 MediaTek | "November 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/November-2025 | 3 November 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

4 CVE Details | "CVE-2025-20725: Out of bounds write vulnerability in MediaTek IMS service" | https://www.cvedetails.com/cve/CVE-2025-20725/ | 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

5 MediaTek | "June 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/June-2025 | 2 June 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

6 MediaTek | "November 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/November-2025 | 3 November 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

7 MediaTek | "June 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/June-2025 | 2 June 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

8 MediaTek | "November 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/November-2025 | 3 November 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

9 MediaTek | "June 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/June-2025 | 2 June 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

10 MediaTek | "November 2025 Product Security Bulletin" | https://corp.mediatek.com/product-security-bulletin/November-2025 | 3 November 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

11 National Vulnerability Database (NVD) | "CVE-2025-20678 Detail" | https://nvd.nist.gov/vuln/detail/CVE-2025-20678 | 1 June 2025 | Accessed on 20 January 2026 | The source is publicly available information and does not contain classification markings

12 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

13 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

14 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

15 ASSET Research Group | "5Ghoul disclosure" | https://asset-group.github.io/disclosures/5ghoul/ | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

16 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

17 ASSET Research Group | "5Ghoul 5G NR attacks (PoC and fuzzer)" | https://github.com/asset-group/5ghoul-5g-nr-attacks | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

18 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

19 ASSET Research Group | "5Ghoul 5G NR attacks (PoC and fuzzer)" | https://github.com/asset-group/5ghoul-5g-nr-attacks | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

20 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

21 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

22 M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan | "5Ghoul: Unleashing Chaos on 5G Edge Devices via Stateful Multi-layer Fuzzing" | https://www.computer.org/csdl/journal/tq/5555/01/11045988/27Mq8MDTqbS | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

23 ASSET Research Group | "5Ghoul 5G NR attacks (PoC and fuzzer)" | https://github.com/asset-group/5ghoul-5g-nr-attacks | 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

24 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

25 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

26 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

27 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

28 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

29 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

30 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

31 A. Chen, R. Preatoni, A. Brighente, M. Conti, and C. Nita-Rotaru | "Cross-Service Token: Finding Attacks in 5G Core Networks" | https://arxiv.org/abs/2509.08992 | 10 September 2025 | Accessed on 14 January 2026 | The source is publicly available information and does not contain classification markings

32 Android Open Source Project | "Android Security Bulletin - August 2025" | https://source.android.com/docs/security/bulletin/2025-08-01 | 4 August 2025; updated 11 September 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

33 Cybersecurity and Infrastructure Security Agency (CISA) | "CISA Adds Three Known Exploited Vulnerabilities to Catalog" | https://www.cisa.gov/news-events/alerts/2025/06/03/cisa-adds-three-known-exploited-

vulnerabilities-catalog | 3 June 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

34 S. Fadilpasic | "Google urgently patches major Qualcomm security flaw hitting Android phones - so make sure you update now" | https://www.techradar.com/pro/security/google-patches-major-qualcomm-security-flaw-hitting-android-phones-heres-what-we-know | 6 August 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

35 Android Open Source Project | "Android Security Bulletin - August 2025" | https://source.android.com/docs/security/bulletin/2025-08-01 | 4 August 2025; updated 11 September 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

36 S. Fadilpasic | "Google urgently patches major Qualcomm security flaw hitting Android phones - so make sure you update now" | https://www.techradar.com/pro/security/google-patches-major-qualcomm-security-flaw-hitting-android-phones-heres-what-we-know | 6 August 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

37 Cybersecurity and Infrastructure Security Agency (CISA) | "CISA Adds Three Known Exploited Vulnerabilities to Catalog" | https://www.cisa.gov/news-events/alerts/2025/06/03/cisa-adds-three-known-exploited-vulnerabilities-catalog | 3 June 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

38 S. Fadilpasic | "Google urgently patches major Qualcomm security flaw hitting Android phones - so make sure you update now" | https://www.techradar.com/pro/security/google-patches-major-qualcomm-security-flaw-hitting-android-phones-heres-what-we-know | 6 August 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

39 National Vulnerability Database (NVD) | "CVE-2025-21479 Detail" | https://nvd.nist.gov/vuln/detail/CVE-2025-21479 | 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

40 National Vulnerability Database (NVD) | "CVE-2025-27038 Detail" | https://nvd.nist.gov/vuln/detail/CVE-2025-27038 | 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

41 Android Open Source Project | "Android Security Bulletin - August 2025" | https://source.android.com/docs/security/bulletin/2025-08-01 | 4 August 2025; updated 11 September 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings

42 Android Open Source Project | "Android Security Bulletin - August 2025" | https://source.android.com/docs/security/bulletin/2025-08-01 | 4 August 2025; updated 11 September 2025 | Accessed on 9 January 2026 | The source is publicly available information and does not contain classification markings