I. Conclusion

This paper analyzed the 2025 WhatsApp–ImageIO zero-click exploit chain (CVE-2025-55177 + CVE-2025-43300), which compromised the mobile devices of fewer than 200 targeted individuals without any user interaction. Through a three-axis framework (root cause, patch, chain position), we reconstructed how a WhatsApp linked-device authorization bypass (CWE-863) delivered a crafted DNG image to Apple's ImageIO framework, where a two-byte inconsistency between TIFF metadata and an embedded JPEG marker triggered a heap out-of-bounds write (CWE-787) leading to remote code execution.

Three findings emerge. First, the fundamental exploitation primitive—a heap buffer overflowed into an adjacent function pointer—is identical to the one demonstrated in the educational Phoenix `heap-two` exercise. The difference between a textbook CTF exercise and a production zero-click chain is engineering (heap grooming, ASLR bypass, PAC bypass), not mechanism. Second, the 2025 chain reproduces the architectural pattern of FORCEDENTRY (2021) with different components—a different messenger, a different parser, a different image format—but the same structural vulnerability. The recurrence across four years and two independent ecosystems suggests that the pattern is inherent to the current architecture of media processing on mobile platforms, not an isolated accident. Third, the deployed mitigation stack (ASLR, stack canaries, sandboxing, PAC) addresses symptoms rather than the root cause: none of these defenses prevent the out-of-bounds write itself.

We recommend two structural interventions. The near-term priority is incremental rewriting of high-exposure C/C++ parsers (ImageIO, CoreGraphics, and their Android equivalents) in memory-safe languages such as Rust or Swift. The longer-term intervention is deployment of hardware-enforced memory tagging (ARM MTE) on iOS, which would make heap overflows detectable at the granule level regardless of the implementation language.

Future work should track whether the "delivery + parser" pattern continues to appear in newly disclosed zero-click chains, and should extend the Phoenix-to-CVE pedagogical bridge to additional vulnerability classes (use-after-free, type confusion) as suitable educational exercises become available.