วันที่ 13 พฤศจิกายน 2568

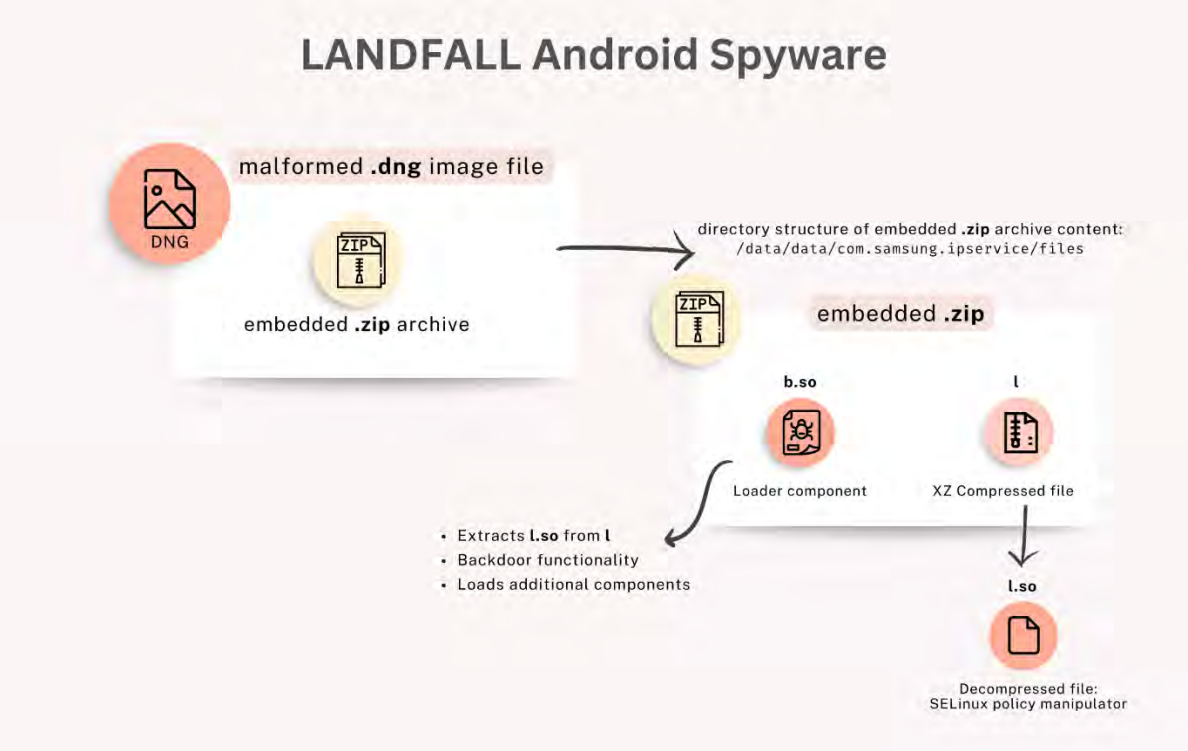
ช่องโหว่บนมือถือ Samsung ถูกใช้แบบ Zero-Day เพื่อติดตั้งสปายแวร์ Android ชื่อ LANDFALL

ช่องโหว่ความปลอดภัยที่ได้รับการแก้ไขแล้วในอุปกรณ์ Samsung Galaxy เคยถูกใช้เป็นช่องโหว่แบบ Zero-Day เพื่อส่งสปายแวร์ Android ระดับ “เชิงพาณิชย์” ชื่อ LANDFALL ในการโจมตีแบบเจาะจงในตะวันออกกลาง โดยนักวิจัยได้ย้อนรอยหลักฐานการโจมตีไปตั้งแต่ช่วงกลางปี 2024

ช่องโหว่ Zero-Day ใน Samsung Galaxy (CVE-2025-21042)

การโจมตีนี้เกี่ยวข้องกับการใช้ประโยชน์จากช่องโหว่ CVE-2025-21042 (คะแนน CVSS: 8.8) ซึ่งเป็นช่องโหว่แบบ “out-of-bounds write” ภายในส่วนประกอบ libimagecodec.quram.so ที่อาจทำให้ผู้โจมตีจากระยะไกลสามารถรันโค้ดได้ตามต้องการ ตามข้อมูลจากทีม Unit 42 ของ Palo Alto Networks

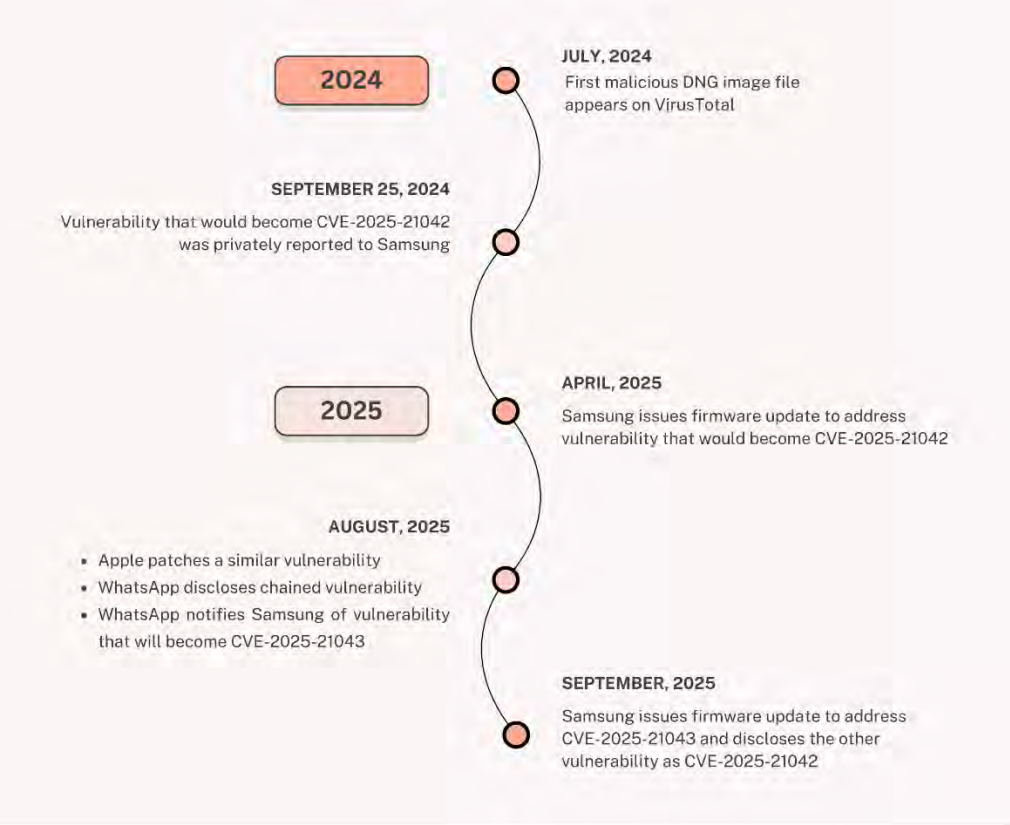
- การโจมตีจริง: Unit 42 ยืนยันว่า ช่องโหว่นี้ถูกใช้โจมตีจริงในสภาพแวดล้อมจริง ก่อนที่ Samsung จะออกแพตช์แก้ไขในเดือนเมษายน 2025
- การเชื่อมโยงกับช่องโหว่อื่น: เหตุการณ์นี้เกิดขึ้นหลังจากในเดือนกันยายน 2025 Samsung เปิดเผยว่ามีช่องโหว่อีกช่องในไลบรารีเดียวกัน (CVE-2025-21043, คะแนน CVSS: 8.8) ที่ถูกใช้โจมตีในโลกจริงแบบ Zero-Day เช่นกัน
- เป้าหมาย: ผู้ที่ตกเป็นเป้าหมายในการโจมตีนี้ (ติดตามในชื่อ CL-UNK-1054) อยู่ในประเทศ อิรัก, อิหร่าน, ตุรกี, และโมร็อกโก ตามข้อมูลจากการส่งตัวอย่างใน VirusTotal
- อุปกรณ์เป้าหมาย: สปายแวร์นี้ถูกออกแบบมาให้มุ่งเป้าเฉพาะอุปกรณ์ Samsung Galaxy รุ่นเรือธง ได้แก่ Galaxy S22, S23, และ S24 รวมถึง Z Fold 4 และ Z Flip 4



กลไกการโจมตี LANDFALL ผ่านไฟล์ DNG

มีการประเมินว่าการโจมตีอาจเกิดขึ้นผ่านการส่งภาพที่เป็นอันตรายผ่านแอป WhatsApp ในรูปแบบไฟล์ DNG (Digital Negative) โดยมีหลักฐานของตัวอย่าง LANDFALL ย้อนหลังไปถึงวันที่ 23 กรกฎาคม 2024

- หลักฐานการโจมตี: พบไฟล์ DNG ที่มีชื่ออย่าง “WhatsApp Image 2025-02-10 at 4.54.17 PM.jpeg” (หลักฐานล่าสุด) และ “IMG-20240723-WA0000.jpg” (หลักฐานย้อนหลัง)
- Zero-Click? แม้ Unit 42 จะระบุว่าชุดการโจมตีอาจใช้วิธี “zero-click” เพื่อกระตุ้นช่องโหว่ แต่ปัจจุบันยังไม่มีหลักฐานยืนยันว่ามีการโจมตีแบบนั้นเกิดขึ้นจริง
- การเชื่อมโยงกับ iOS: ควรสังเกตว่าช่วงเวลาเดียวกัน WhatsApp ได้เปิดเผยช่องโหว่ในแอปเวอร์ชัน iOS และ macOS (CVE-2025-55177, CVSS: 5.4) ที่ถูกเชื่อมต่อเข้ากับช่องโหว่ CVE-2025-43300 (CVSS: 8.8) ในระบบ iOS, iPadOS และ macOS ของ Apple เพื่อมุ่งเป้าผู้ใช้น้อยกว่า 200 รายในแคมเปญที่ซับซ้อน



การติดตั้งและการคงอยู่ถาวรทางเทคนิค

1. การฝังไฟล์: การวิเคราะห์ไฟล์ DNG เผยว่าไฟล์เหล่านี้มี ไฟล์ ZIP ฝังอยู่ตอนท้าย โดยช่องโหว่ถูกใช้เพื่อดึงไฟล์ “shared object” จาก ZIP ออกมารันสปายแวร์
2. การยกระดับสิทธิ์: ภายใน ZIP ยังมี “shared object” อีกไฟล์ที่ออกแบบมาเพื่อแก้ไข นโยบาย SELinux ของอุปกรณ์ เพื่อให้ LANDFALL มีสิทธิ์สูงขึ้นและสามารถคงอยู่ในระบบได้
3. การสื่อสาร C2: ไฟล์ shared object ที่ใช้โหลด LANDFALL ยังมีการสื่อสารกับเซิร์ฟเวอร์สั่งการ (C2) ผ่าน HTTPS เพื่อเข้าสู่กระบวนการ beaconing loop และรับเพย์โหลดในขั้นตอนถัดไปมารันต่อ
4. ความสามารถ: LANDFALL เป็น เฟรมเวิร์กสปายแวร์แบบโมดูลาร์ และทำหน้าที่เป็นเครื่องมือสอดแนมเต็มรูปแบบที่สามารถเก็บข้อมูลสำคัญ เช่น การบันทึกเสียงจากไมโครโฟน, ตำแหน่งที่ตั้ง, รูปภาพ, รายชื่อผู้ติดต่อ, ข้อความ SMS, ไฟล์ต่าง ๆ และบันทึกการโทร

ความคล้ายคลึงกับ Stealth Falcon และ CISA KEV

- การเชื่อมโยงผู้โจมตี: Unit 42 ระบุว่าโครงสร้างพื้นฐาน C2 และรูปแบบการลงทะเบียนโดเมนของ LANDFALL มีความคล้ายคลึงกับของกลุ่ม Stealth Falcon (หรือ FruityArmor)
- การแจ้งเตือน CISA: เมื่อวันที่ 10 พฤศจิกายน 2025 หน่วยงานด้านความมั่นคงไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) ได้เพิ่ม CVE-2025-21042 ลงในแค็ตตาล็อกช่องโหว่ที่ถูกใช้โจมตีจริง (Known Exploited Vulnerabilities – KEV) และกำหนดให้หน่วยงานรัฐบาลพลเรือนของสหรัฐฯ (FCEB) ต้องแก้ไขช่องโหว่นี้ภายในวันที่ 1 ธันวาคม 2025

Itay Cohen จาก Unit 42 กล่าวว่า: "เราไม่เชื่อว่าช่องโหว่นี้ยังถูกใช้อยู่ในตอนนี้ เนื่องจาก Samsung ได้แก้ไขแล้วในเดือนเมษายน 2025... แต่ยังมีบางโครงสร้างพื้นฐานที่อาจเชื่อมโยงกับ LANDFALL ซึ่งยังคงออนไลน์อยู่ บ่งชี้ว่าผู้โจมตีอาจยังคงมีกิจกรรมต่อเนื่อง”

ข้อมูลอ้างอิง

Nov 7, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/11/samsung-zero-click-flaw-exploited-to.html