TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Google แก้ไขช่องโหว่ Zero-Day ใน Android

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี Google แก้ไขช่องโหว่ Zero-Day ใน Android

Google ได้ออกอัปเดตความปลอดภัย Android ประจำเดือนกุมภาพันธ์ 2025 โดยแก้ไข 48 ช่องโหว่ รวมถึงช่องโหว่ Zero-Day CVE-2024-53104 ซึ่งถูกใช้ประโยชน์ในการโจมตี โดยเป็นช่องโหว่การยกระดับสิทธิ์ (Privilege Escalation) ใน Kernel's USB Video Class (UVC) driver ที่ช่วยให้ผู้โจมตีสามารถเพิ่มสิทธิ์ในระบบได้ ซึ่งเกิดจากการประมวลผล UVC_VS_UNDEFINED Frame ที่ผิดพลาด ที่อาจนำไปสู่การโจมตีแบบ Arbitrary Code Execution หรือ Denial-of-Service

Google ได้ออกแพตช์ความปลอดภัยสองชุดคือ 2025-02-01 และ 2025-02-05 และแก้ไขช่องโหว่ระดับ Critical ที่หมายเลข CVE-2024-45569 มีคะแนน CVSS 9.8 ใน Qualcomm's WLAN component ซึ่งเป็นปัญหาการ Memory Corruption ระหว่างประมวลผลเฟรม ML IE นอกจากนี้เมื่อเดือนพฤศจิกายน 2024 Google ยังแก้ไขช่องโหว่ Zero-Day ที่หมายเลข CVE-2024-43047 และ CVE-2024-43093 ที่ถูกใช้ประโยชน์ในการโจมตีและแม้ว่า Google จะไม่ได้เปิดเผยรายละเอียดของการโจมตี แต่แนะนำให้ผู้ใช้งาน Android อัปเดตล่าสุดโดยเร็ว เพื่อป้องกันความเสี่ยงจากช่องโหว่ที่อาจถูกใช้ในการโจมตีเพิ่มเติม[1]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้ Android อัปเดตระบบเป็นเวอร์ชันล่าสุดเพื่อป้องกันการโจมตี และลดความเสี่ยงจากช่องโหว่อื่นๆ ที่อาจถูกใช้ประโยชน์เพิ่มเติมและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://securityaffairs.com/173812/hacking/google-android-kernel-zero-day-flaw.html