ประจำวันจันทร์ที่ 15 สิงหาคม 2565

โทรศัพท์ Xiaomi ที่มีชิป MediaTek พบว่ามีความเสี่ยงต่อการปลอมแปลงการชำระเงิน

มีการระบุข้อบกพร่องด้านความปลอดภัยใน Xiaomi รุ่น Redmi Note 9T และ Redmi Note 11 ซึ่งสามารถใช้เพื่อปิดใช้งานกลไกการชำระเงินผ่านมือถือ และปลอมแปลงธุรกรรมผ่านแอพ Android ปลอมที่ติดตั้งบนอุปกรณ์ได้ โดย Check Point กล่าวว่าพบข้อบกพร่องในอุปกรณ์ที่ทำงานโดยชิปเซ็ต MediaTek ในระหว่างการวิเคราะห์ความปลอดภัยของ "Kinibi" Trusted Execution Environment (TEE) ของผู้ผลิตโทรศัพท์มือถือจากจีน โดย TEE หมายถึงวงล้อมที่ปลอดภัยภายในโปรเซสเซอร์หลักที่ใช้ในการประมวลผลและจัดเก็บข้อมูลที่ละเอียดอ่อน เช่น คีย์การเข้ารหัส เพื่อให้มั่นใจในการรักษาข้อมูลความลับ

บริษัทรักษาความปลอดภัยทางไซเบอร์ของอิสราเอลพบว่าแอปที่เชื่อถือได้ในอุปกรณ์ Xiaomi สามารถดาวน์เกรดได้เนื่องจากไม่มีการควบคุมการอัพเวอร์ชันใด ๆ ทำให้ผู้โจมตีสามารถแทนที่แอปเวอร์ชันใหม่ ทั้งนี้ Slava Makkaveev นักวิจัยของ Check Point กล่าวในรายงานที่แบ่งปันกับ The Hacker News ว่า ผู้โจมตีสามารถเลี่ยงการแก้ไขด้านความปลอดภัยของ Xiaomi หรือ MediaTek ในแอปที่เชื่อถือได้โดยดาวน์เกรดให้เป็นเวอร์ชันที่ไม่ได้รับการแก้ไข

นอกจากนี้ ยังมีการระบุช่องโหว่หลายจุดใน "thhadmin" ซึ่งเป็นแอปที่เชื่อถือได้ แอปนี้มีหน้าที่ในการจัดการความปลอดภัย ซึ่งอาจถูกนำไปใช้ในทางที่ผิดด้วยแอปที่เป็นอันตราย เพื่อทำให้คีย์ที่เก็บไว้รั่วไหลหรือเพื่อรันโค้ดโดยอำเภอใจ

หลังจากการเปิดเผย Xiaomi ได้กล่าวถึงช่องโหว่ CVE-2020-14125 ซึ่งเป็นส่วนหนึ่งของการอัปเดตที่ได้เผยแพร่ไปเมื่อวันที่ 6 มิถุนายน 2022 ว่า "ปัญหาการปรับลดรุ่นซึ่ง Xiaomi ยืนยันว่ากำลังได้รับการแก้ไขอยู่ในขณะนี้"

ที่มาของข่าว : https://thehackernews.com/2022/08/xiaomi-phones-with-mediatek-chips-found.html