ประจำวันจันทร์ที่ 13 มิถุนายน 2565

นักวิจัย MIT ค้นพบข้อบกพร่องใหม่ในชีพียู Apple M1 ที่ไม่สามารถแก้ไขได้

นักวิจัยของ MIT พบการโจมตีด้วยฮาร์ดแวร์รูปแบบใหม่ที่เรียกว่า PACMAN ได้แสดงให้เห็นในชิปเซ็ตโปรเซสเซอร์ M1 ของ Apple ซึ่งอาจทำให้ผู้ประสงค์ร้ายสามารถเรียกใช้โค้ดโดยอำเภอใจบนระบบ macOS ได้ โดยช่องโหว่นี้มีรากฐานมาจากรหัสตรวจสอบความถูกต้องของตัวชี้ (PACs) ซึ่งเป็นแนวป้องกันที่นำมาใช้ในสถาปัตยกรรม arm64e ที่มีจุดมุ่งหมายเพื่อตรวจจับและป้องกันการเปลี่ยนแปลงที่ไม่คาดคิดของพอยน์เตอร์ ซึ่งเป็นวัตถุที่เก็บที่อยู่หน่วยความจำไว้ในหน่วยความจำ

PAC มีเป้าหมายเพื่อแก้ปัญหาทั่วไปในความปลอดภัยของซอฟต์แวร์ เช่น ช่องโหว่หน่วยความจำเสียหาย ซึ่งมักถูกโจมตีโดยการเขียนทับข้อมูลการควบคุมในหน่วยความจำ (เช่น พอยน์เตอร์) เพื่อเปลี่ยนเส้นทางการเรียกใช้โค้ดไปยังตำแหน่งที่ผู้โจมตีควบคุมโดยอำเภอใจ

โดยสรุปวิธีการโจมตีทำให้สามารถแยกแยะระหว่าง PAC ที่ถูกต้องและแฮชที่ไม่ถูกต้อง อนุญาตให้ผู้กระทำผิดสามารถ " brute-force ค่า PAC ที่ถูกต้อง ในขณะที่ระงับการหยุดทำงาน และสร้างการโจมตีแบบควบคุมการไหลของการควบคุมบน PA ที่เปิดใช้งาน โปรแกรมเหยื่อหรือระบบปฏิบัติการ” ในส่วนของการป้องกันข้อขัดข้องนั้นสำเร็จ เนื่องจากค่า PAC แต่ละค่าถูกคาดเดาโดยคาดเดาโดยใช้ประโยชน์จากช่องสัญญาณด้านข้างที่อิงตามเวลาผ่านการแปล look-aside buffer (TLB) โดยใช้การโจมตีแบบ Prime +Probe ซึ่งนักวิจัยสรุปว่า "การโจมตีนี้มีนัยสำคัญสำหรับนักออกแบบที่ต้องการใช้โปรเซสเซอร์ในอนาคตที่มีการรับรองความถูกต้องของพอยท์เตอร์ และมีความหมายกว้างๆ ต่อความปลอดภัยของระบบพื้นฐานความสมบูรณ์ของกระแสการควบคุมในอนาคต"

ที่มาของข่าว : https://thehackernews.com/2022/06/mit-researchers-discover-new-flaw-in.html