เอกสารการแจ้งเตือนกรณี AMD แก้ไขช่องโหว่ที่ทำให้สามารถโหลดไมโครโค้ดอันตรายได้

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี AMD แก้ไขช่องโหว่ที่ทำให้สามารถโหลดไมโครโค้ดอันตรายได้

AMD ได้ออกแพตช์เพื่อแก้ไขช่องโหว่ CVE-2024-56161 (มีคะแนน CVSS 7.2) ที่ถูกค้นพบโดยนักวิจัยจาก Google โดยช่องโหว่นี้ทำให้ผู้โจมตีที่มีสิทธิ์ระดับผู้ดูแลระบบสามารถโหลดไมโครโค้ดอันตรายเข้าสู่ CPU ได้ ซึ่งส่งผลกระทบต่อ Secure Encrypted Virtualization (SEV) เป็นเทคโนโลยีที่ใช้ปกป้องหน่วยความจำของเครื่องเสมือน (VM) จากการเข้าถึงโดยไม่ได้รับอนุญาต

ช่องโหว่นี้เกิดจากการใช้ฟังก์ชันแฮชที่ไม่ปลอดภัยในการตรวจสอบลายเซ็นไมโครโค้ดทำให้ผู้โจมตีสามารถสร้างไมโครโค้ดอันตรายเพื่อโจมตี CPU Zen 1 ถึง Zen 4 และอาจเกิดความเสียหายกับระบบที่ใช้ SEV-SNP ซึ่งเป็นเวอร์ชันล่าสุดของการประมวลผลแบบ Confidential Computing เพื่อป้องกันปัญหา AMD ได้ออกไมโครโค้ดและเฟิร์มแวร์อัปเดต พร้อมแนะนำให้ทำการอัปเดต BIOS และรีบูตเครื่อง

นักวิจัยได้จัดทำ Proof of Concept (PoC) เพื่อแสดงให้เห็นว่าช่องโหว่นี้สามารถถูกใช้โจมตี CPU AMD Zen 1 ถึง Zen 4 และอาจส่งผลกระทบต่อการประมวลผลแบบ Confidential Computing และระบบ Dynamic Root of Trust Measurement ทั้งนี้ AMD แนะนำให้ผู้ใช้และผู้ดูแลระบบดำเนินการอัปเดตระบบทันที เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านช่องโหว่นี้[1]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://securityaffairs.com/173831/security/amd-flaw-allowed-load-malicious-microcode.html