แจ้งเตือน

Critical

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Google ออก Security Patch แก้ไขช่องโหว่ Zero Day ในระบบปฏิบัติการ Android และ AMD ออก Security Patch แก้ไขช่องโหว่เครื่อง Virtual Machine

วันที่แจ้งเตือน 14 กุมภาพันธ์ 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (“สำนักงาน ก.ล.ต.”) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (“TCM-CERT”) ร่วมกับศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามเกี่ยวกับการโจมตีทางไซเบอร์ โดยพบว่า

1. Google ได้ออกแพตช์แก้ไขช่องโหว่ความมั่นคงปลอดภัยในระบบปฏิบัติการ Android จำนวน 48 รายการ รวมถึง (1) ช่องโหว่ Zero Day ในส่วนประกอบ USB Video Class (UVC) driver ของ Android Kernel (CVE-2024-53104) ทำให้ผู้ไม่ประสงค์ดีสามารถยกระดับสิทธิ์ (Privilege Escalation) และเข้าควบคุมระบบได้ (2) ช่องโหว่ใน WLAN component ของ Qualcomm (CVE-2024-45569) ทำให้เกิด Memory Corruption ระหว่างประมวลผลเฟรม ML IE และอาจนำไปสู่การโจมตีแบบ Arbitrary Code Execution หรือ Denial-of-Service ส่งผลให้เกิดการหยุดทำงานของระบบ และการรั่วไหลของข้อมูลที่เป็นความลับได้ และ (3) ช่องโหว่ Zero-Day (CVE-2024-43047 และ CVE-2024-43093) ที่ถูกใช้ประโยชน์ในการโจมตี ทั้งนี้ Google แนะนำให้ผู้ใช้งาน Android ติดตั้ง Security Patch เวอร์ชันล่าสุดสำหรับอุปกรณ์ที่มีการใช้งานตรวจสอบและอัปเดตระบบปฏิบัติการ Android ให้เป็นเวอร์ชันล่าสุด จำกัดการเข้าถึง USB และการเชื่อมต่อกับอุปกรณ์ภายนอกที่ไม่จำเป็น เพิ่มการตรวจสอบและเฝ้าระวังการใช้งานที่ผิดปกติ รวมถึงกิจกรรมที่เกี่ยวข้องกับการยกระดับสิทธิ์ และจัดทำแผนรับมือเหตุการณ์ฉุกเฉิน กรณีพบการโจมตีเพื่อป้องกันความเสี่ยงจากช่องโหว่ที่อาจถูกใช้ในการโจมตีเพิ่มเติม

2. AMD ได้ออก Patch เพื่อแก้ไขช่องโหว่ที่มีความเสี่ยงสูง (CVE-2024-56161) ในระบบ Secure Encrypted Virtualization (SEV) ซึ่งเป็นฟีเจอร์ที่ใช้ปกป้องหน่วยความจำของเครื่องเสมือน Virtual Machine (VM) จากการเข้าถึงโดยไม่ได้รับอนุญาตโดยช่องโหว่นี้เกิดจากการตรวจสอบลายเซ็นดิจิทัลที่ไม่สมบูรณ์ในส่วนของ CPU ROM microcode patch loader ทำให้ผู้ไม่ประสงค์ดีใช้สิทธิ์ High Privilege ในการหลบเลี่ยงการรักษาความมั่นคงปลอดภัยและเข้าถึงระบบ ทำการโหลด microcode ที่เป็นอันตรายเข้าสู่ระบบได้ ส่งผลให้สูญเสียการรักษาความลับและความถูกต้องของข้อมูลใน VM โดยผลิตภัณฑ์ที่ได้รับผลกระทบครอบคลุม CPU รุ่น AMD EPYC ได้แก่ (1) AMD EPYC 7001 Series (Naples) (2) 7002 Series (Rome) (3) 7003 Series (Milan/Milan-X) และ (4) 9004 Series (Genoa/Genoa-X/Bergamo/Siena) ทั้งนี้ ผู้ประกอบธุรกิจควรพิจารณาดำเนินการติดตั้ง microcode update ล่าสุดสำหรับระบบที่ได้รับผลกระทบทั้งหมด อัปเดต SEV firmware สำหรับระบบที่ใช้ SEV-SNP อัปเดต BIOS ของระบบและทำการรีบูต เพื่อให้การป้องกันมีผลสมบูรณ์ และปฏิบัติตามแนวทางการป้องกันการโจมตีแบบ cache-based side-channel ตามที่ AMD แนะนำ

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 6 กุมภาพันธ์ 2568
2. https://www.bleepingcomputer.com/news/security/google-fixes-android-kernel-zero-day-exploited-in-attacks/
3. https://www.bleepingcomputer.com/news/security/amd-fixes-bug-that-lets-hackers-load-malicious-microcode-patches/
4. https://nvd.nist.gov/vuln/detail/cve-2024-43047
5. https://nvd.nist.gov/vuln/detail/CVE-2024-43093
6. https://nvd.nist.gov/vuln/detail/CVE-2024-45569
7. https://nvd.nist.gov/vuln/detail/CVE-2024-53104
8. https://nvd.nist.gov/vuln/detail/CVE-2024-56161