รู้จักกับ Meltdown และ Spectre ช่องโหว่บนเครื่องคอมพิวเตอร์รุ่นใหม่ (1/2)

TLP:WHITE

เผยแพร่วันที่ 6 มกราคม 2561

เปิดฉากปีใหม่ ในวันที่ 3 มกราคม 2561 มีการรายงานช่องโหว่ด้านความปลอดภัยที่มีผลกระทบกับ ซีพียู รุ่นใหม่เกือบทุกรุ่น ด้วยการอาศัยช่องโหว่นี้ผู้ประสงค์ร้ายจะสามารถสร้างโปรแกรมเพื่อขโมยข้อมูลของโปรแกรมอื่นที่กำลังประมวลผลอยู่ในขณะนั้น ไม่ว่าจะเป็นข้อมูลรหัสผ่าน ข้อมูลกุญแจลับ โทเค็น อีเมล หรือแม้กระทั่งข้อมูลสำคัญทางธุรกิจ ซึ่งโดยปกติแล้วระบบปฏิบัติการจะไม่อนุญาตให้เข้าถึงข้อมูลของโปรแกรมอื่นได้

เทคนิคการโจมตี

การเพิ่มความเร็วในการประมวลผลของคอมพิวเตอร์ในยุคที่ซีพียูรุ่นใหม่มีประสิทธิภาพในการทำงานที่สูงนั้น เทคนิคหนึ่งที่ใช้กันคือการทำ speculative execution หรือ การคาดเดาและโหลดชุดคำสั่งที่จะใช้งานล่วงหน้า ซึ่งหากการคาดเดาทำได้อย่างถูกต้องแม่นยำจะเป็นการเพิ่มประสิทธิภาพการทำงานอย่างมาก แต่หากการคาดเดาไม่ถูกต้องก็จะทำการโหลดชุดคำสั่งตามลำดับที่ควรจะเป็นเหมือนเช่นเดิม อย่างไรก็ตามเทคนิคนี้จะสร้างปัญหาด้านความปลอดภัย กล่าวคือการโหลดชุดคำสั่งล่วงหน้ารวมถึงข้อมูลที่ต้องใช้ในการทำงานของชุดคำสั่งก่อนช่วงเวลาที่จำเป็นต้องใช้งานมาไว้ในหน่วยความจำ จะทำให้สามารถเขียนโปรแกรมเข้าไปขโมยข้อมูลดังกล่าวได้ ซึ่งเป็นเทคนิคของการโจมตีช่องโหว่ Meltdown และ Spectre **จุดแตกต่างของช่องโหว่ Meltdown และ Spectre คือระดับที่จะขโมยข้อมูลได้ ซึ่ง Meltdown ลงลึกได้ถึงระบบปฏิบัติการ ส่วน Spectre จะเป็นแอปพลิเคชันที่ทำงานอยู่ในขณะนั้น**

ทั้งนี้การจะโจมตีช่องโหว่นี้ผู้ประสงค์ร้ายจำเป็นต้องหาวิธีลงโปรแกรมบนเครื่องเป้าหมายให้ได้ก่อน จึงจะสามารถรันโปรแกรมและใช้ช่องโหว่ Meltdown หรือ Spectre ในการขโมยข้อมูล ซึ่งอาจจะใช้วิธีการฝังโปรแกรมบนเว็บไซต์ ส่งมัลแวร์ทางอีเมล หรือ Thumb Drive ปัจจุบันยังไม่มีข้อมูลชัดเจนว่ามีการใช้เทคนิคใดบ้าง เพียงแค่พบรูปแบบของการเขียนโค้ดเป็น JavaScript ฝังอยู่ในเว็บไซต์ นอกจากนั้นยังไม่ได้รับรายงานงานว่ามีการส่งโปรแกรมแบบรีโมทและยังไม่พบข้อมูลที่ระบุวิธีการส่งข้อมูลที่ขโมยได้ออกไป

อุปกรณ์ที่ได้รับผลกระทบ

มุ่งเน้นเรื่องความปลอดภัย สร้างความมั่นใจ ให้ความเห็นอย่างเป็นกลาง

TB-CERT
Thailand Banking Sector CERT

รู้จักกับ Meltdown และ Spectre ช่องโหว่บนเครื่องคอมพิวเตอร์รุ่นใหม่ (2/2)

TLP:WHITE

เผยแพร่วันที่ 6 มกราคม 2561

ข้อแนะนำ

1. ประเมินความเสี่ยงของระบบงานเพื่อจัดลำดับความสำคัญในการทดสอบและติดตั้งแพตช์บนเครื่องเซิร์ฟเวอร์ โดยต้องพิจารณาการควบคุมการเชื่อมต่อของเซิร์ฟเวอร์ประกอบด้วย ควรจะให้ลำดับการติดตั้งแพตช์สำหรับเซิรฟ์เวอร์ที่มีการเชื่อมต่ออินเตอร์เน็ตหรือควบคุมการเชื่อมต่ออินเตอร์เน็ตให้รัดกุมมากขึ้น
2. ทดสอบและติดตั้งแพตช์ (Patch) ปัจจุบันเจ้าของผลิตภัณฑ์ทยอยประกาศแจ้งเตือนให้ติดตั้งแพตช์เพื่อควบคุมความเสี่ยงนี้ อย่างไรก็ตามแพตช์ดังกล่าวอาจจะมีผลกระทบต่อประสิทธิภาพการทำงานของเครื่อง หรืออาจทำให้ทำงานขัดกับซอฟต์แวร์ Anti-virus ดังนั้นจำเป็นต้องทดสอบการติดตั้งแพตช์ ก่อนนำไปลงใน Production เพื่อไม่ให้ส่งผลกระทบกับบริการ
3. ป้องกันเครื่องคอมพิวเตอร์ที่เชื่อมต่อในองค์กร โดยใช้ proxy ในการควบคุมการเข้าถึงเว็บไซต์ที่มีความเสี่ยง ผู้ดูแลจะต้องยกระดับการเฝ้าระวังให้สูงขึ้นสำหรับเว็บไซต์ที่มีความเสี่ยงสูงโดยเฉพาะเว็บไซต์ที่ถูกพัฒนาด้วย Java Script หากเครื่องที่เข้าถึงอินเตอร์เน็ตจากในองค์กรยังไม่สามารถติดตั้งแพตช์ได้ครบถ้วน
4. ป้องกันเครื่องคอมพิวเตอร์และอุปกรณ์เคลื่อนที่ที่เชื่อมอินเตอร์เน็ตโดยตรง **สำหรับผู้ใช้งานทั่วไป** ให้พิจารณาปิดการใช้งาน Java Script หรือจำกัดให้เข้าถึงเฉพาะเว็บไซต์ที่น่าเชื่อถือได้เป็นพิเศษ (Trusted site) ในช่วงที่ยังไม่ได้ติดตั้งแพตช์
5. ติดตามข้อมูลการประกาศแพตช์จากเจ้าของผลิตภัณฑ์ที่ใช้งานอยู่ รวมถึงติดตามข้อมูลความคืบหน้าของการโจมตีนี้
6. ติดตามสอบถามข้อมูลเรื่องการลงแพตช์หรือมาตรการป้องกันสำหรับผู้ใช้บริการคลาวด์จากผู้ให้บริการ

ข้อควรระวัง

1. ปัจจุบันซอฟต์แวร์ Anti-virus ยังไม่สามารถตรวจจับได้หรือป้องกันช่องโหว่นี้ได้
2. การจะติดตั้งแพตช์อาจจะส่งผลกระทบต่อประสิทธิภาพของเครื่อง หรือขัดกับซอฟต์แวร์ Anti-virus ดังนั้นจำเป็นต้องสอบถามข้อมูลกับบริษัทซอฟต์แวร์ Anti-virus ด้วย

เอกสารอ้างอิง

1. https://meltdownattack.com/
2. https://www.us-cert.gov/ncas/alerts/TA18-004A