วันที่ 25 มิถุนายน 2567

High-Risk Overflow Bug in Intel Chips Likely Impacts 100s of PC Models

Executive Summary

ทางศูนย์ CSOC พบรายงานการแจ้งเตือนเกี่ยวกับช่องโหว่ในโปรเซสเซอร์ของ Intel ที่อาจส่งผลกระทบต่อ PC หลายร้อยรุ่น โดยช่องโหว่นี้เป็นช่องโหว่เก่าที่มีมานาน แต่เพิ่งได้รับการเปิดเผยทำให้เกิดปัญหาในการแก้ไข เนื่องจากปัญหาอยู่ที่ Intel Chips ภายในคอมพิวเตอร์ส่วนบุคคล เครื่องเซิร์ฟเวอร์ และโทรศัพท์มือถือ รวมถึง supply chain ที่มีการค้นพบช่องโหว่ที่มีความเสี่ยงสูงในโปรเซสเซอร์ของ Intel เมื่อเร็วๆ นี้ ที่ระบุเป็น CVE-2024-0762: UEFIcanhazbufferoverflow เป็นการโจมตีในลักษณะของ buffer overflow ที่ส่งผลอย่างมากในอุตสาหกรรมเทคโนโลยี SecureCore Unified Extensible Firmware Interface (UEFI) ของ Phoenix Technologies โดยช่องโหว่นี้ได้ถูกเปิดเผยครั้งแรกในเดือนพฤษภาคม ที่ได้ถูกอธิบายโดยทีมนักวิจัยของ Eclypsium ว่าถูกพบครั้งแรกในเดือนพฤศจิกายน ในขณะที่กำลังวิเคราะห์ UEFI images ในแล็ปท็อป ThinkPad X1 Carbon 7th Gen และ X1 Yoga 4th Gen แต่ปัญหาที่เกิดขึ้นเกิดจากจากการเรียกใช้บริการที่ไม่ปลอดภัยของ runtime GetVariable() ที่ใช้ในการอ่านตัวแปรของ UEFI ซึ่งอาจส่งผลให้ผู้โจมตีป้อนข้อมูลมากเกินไปทำให้เกิด Buffer Overflow ทำผู้โจมตีสามารถใช้ประโยชน์โดยการยกระดับการเข้าถึงและดำเนินการโค้ดในเครื่องเป้าหมายในขณะที่ทำงานอยู่ ยิ่งไปกว่านั้นคือความรุนแรงของบั๊กตัวนี้คือการแพร่กระจายของ Intel Chips ที่เป็นโปรเซสเซอร์ที่ขายทั่วโลก

ปัญหาเกี่ยวกับ UEFI

การโจมตีด้วยมัลแวร์ที่มีประสิทธิภาพและยากที่จะกำจัดใน UEFI และ BIOS ในขณะที่ Firmware เป็นอินเทอร์เฟซเฟิร์มแวร์ที่ควบคุมวิธีการบูตของระบบ Firmware และเป็นโค้ดที่มีสิทธิพิเศษสูงสุดที่รันเมื่อผู้ใช้กดปุ่ม power บนอุปกรณ์ ซึ่งความพิเศษนี้ทำให้ผู้โจมตีจากทั่วโลกให้ความสนใจในช่วงหลายปีที่ผ่านมา ทำให้พวกเขาสามารถได้รับสิทธิ์การเข้าถึงเท่ากับเจ้าของของเครื่องและยังคงอยู่ในระบบได้นานผ่านการรีบูตเพื่อหลีกเลี่ยงจากโปรแกรมรักษาความปลอดภัยที่อาจจับมัลแวร์แบบดั้งเดิมได้ มันอาจดูไร้ประโยชน์ในการโจมตี แต่เป็นประโยชน์มากสำหรับการเข้าถึง Nate Warfiel ผู้อำนวยการฝ่ายวิจัยภัยคุกคามและข่าวกรองของ Eclypsium กล่าวว่าหากคุณสามารถรันโค้ดในระหว่างขั้นตอนการบูตของคอมพิวเตอร์ คุณสามารถแทรกอะไรบางอย่างลงใน boot sector หรือคุณสามารถใช้ช่องโหว่นี้ในการปล่อยมัลแวร์เข้าไปใน Windows ก่อนที่มันจะเริ่มทำงาน กล่าวคือ CodmicStrand UEFI rootkit ที่เพิ่งถูกค้นพบทำให้ UEFIcanhazbufferoverflow เป็นอันตราย โดยช่องโหว่นี้ได้รับคะแนน CVSS : 7.5 แต่อย่างไรก็ตามผู้โจมตีจะต้องสามารถเข้าถึงเครื่องเป้าหมายให้ได้ก่อน นอกจากนี้การโจมตีในกรณีนี้อาจต้องปรับแต่งให้เข้ากับ configuration ของรุ่นคอมพิวเตอร์ที่เป็นเป้าหมายและยกระดับความซับซ้อนของการโจมตีเพื่อเพิ่มความเป็นไปได้ที่จะทำให้ช่องโหว่นี้

รายละเอียดของช่องโหว่โดยสรุป

- ผลิตภัณฑ์ที่ได้รับผลกระทบ: Intel Chips
- หน่วยงานที่ออกคำแนะนำด้านความปลอดภัย: Eclypsium
- ผลกระทบ (Impact): Buffer Overflow, Privilege Escalation, Code Execution

- CVE Names:
    - CVE-2024-0762: UEFIcanhazbufferoverflow CVSS Score: 7.5

คำแนะนำจากศูนย์ CSOC

- ติดตามการประกาศและคำแนะนำจาก Intel เกี่ยวกับการแก้ไขปัญหาและการอัปเดตเฟิร์มแวร์
- ควรตรวจสอบและติดตั้งแพตช์ที่เกี่ยวข้องจากผู้ผลิตระบบปฏิบัติการ
- ใช้ซอฟต์แวร์รักษาความปลอดภัยที่ทันสมัยและอัปเดตอย่างสม่ำเสมอเพื่อตรวจจับและป้องกันการโจมตีที่อาจเกิดขึ้น
- ตรวจสอบและปรับปรุงการตั้งค่าความปลอดภัยของระบบและเครือข่ายเพื่อป้องกันการโจมตี
- การจัดการสิทธิ์การเข้าถึงโดยการกำหนดให้ผู้ใช้งานและโปรแกรมมีสิทธิ์เข้าถึงเฉพาะส่วนที่จำเป็นเท่านั้น

ข้อมูลอ้างอิง

- https://www.darkreading.com/vulnerabilities-threats/high-risk-overflow-bug-in-intel-chips-likely-impacts-100s-of-pc-models