ประจำวันอังคารที่ 13 กันยายน 2565

ช่องโหว่เฟิร์มแวร์ในคอมพิวเตอร์ HP หลายรุ่น ไม่ได้รับการแก้ไขมานานกว่าหนึ่งปี

ช่องโหว่ของเฟิร์มแวร์ที่มีความรุนแรงสูงจำนวน 6 รายการที่ส่งผลกระทบต่ออุปกรณ์ HP ยังคงรอการแพตช์ แม้ว่าจะได้มีการเปิดเผยข้อมูลบางส่วนต่อสาธารณะตั้งแต่เดือนกรกฎาคม 2021 ช่องโหว่ของเฟิร์มแวร์นั้นอันตรายเป็นพิเศษเพราะสามารถนำไปสู่การติดมัลแวร์

นักวิจัยจาก Binarly ได้รายงานการพบช่องโหว่ 3 รายการ ในเดือนกรกฎาคม 2021 และอีก 3 รายการในเดือนเมษายน 2022 โดยช่องโหว่ที่ทีมวิจัยด้านความปลอดภัยของ Binarly ได้ค้นพบเมื่อเร็วๆ นี้ คือปัญหาความเสียหายของหน่วยความจำ SMM (System Management Module) ทั้งหมดที่นำไปสู่การใช้รหัสตามอำเภอใจ ซึ่ง SMM เป็นส่วนหนึ่งของเฟิร์มแวร์ UEFI ที่มีฟังก์ชันทั่วทั้งระบบ เช่น การควบคุมฮาร์ดแวร์ระดับต่ำและการจัดการพลังงาน

ช่องโหว่ทั้ง 6 รายการที่ถูกค้นพบจาก Binarly มีดังนี้
- CVE-2022-23930 – buffer overflow แบบ Stack ที่นำไปสู่การเรียกใช้โค้ดตามอำเภอใจ (คะแนน CVSS v3: 8.2 สูง)
- CVE-2022-31644 – Out-of-bounds write on CommBuffer ซึ่งอนุญาตให้ข้ามการตรวจสอบความถูกต้อง (คะแนน CVSS v3: 7.5 สูง)
- CVE-2022-31645 – Out-of-bounds write on CommBuffer โดยอิงจากการไม่ตรวจสอบขนาดของตัวชี้ที่ส่งไปยังตัวจัดการ SMI (คะแนน CVSS v3: 8.2 สูง)
- CVE-2022-31646 – Out-of-bounds write อิงตามฟังก์ชัน API การจัดการหน่วยความจำโดยตรง ซึ่งนำไปสู่การยกระดับสิทธิ์และการใช้รหัสตามอำเภอใจ (คะแนน CVSS v3: 8.2 สูง)
- CVE-2022-31640 – การตรวจสอบอินพุตที่ไม่เหมาะสมทำให้ผู้โจมตีสามารถควบคุมข้อมูล CommBuffer และเปิดเส้นทางสู่การแก้ไขที่ไม่จำกัด (คะแนน CVSS v3: 7.5 สูง)
- CVE-2022-31641 – ช่องโหว่ Callout ในตัวจัดการ SMI ที่นำไปสู่การใช้รหัสตามอำเภอใจ (คะแนน CVSS v3: 7.5 สูง)

โดย HP ได้ออกคำแนะนำด้านความปลอดภัยสามรายการเพื่อรับทราบถึงช่องโหว่ดังกล่าว พร้อมกับการอัปเดต BIOS เพื่อแก้ไขปัญหาสำหรับบางรุ่นที่ได้รับผลกระทบจากช่องโหว่ CVE-2022-23930 ซึ่งได้รับการแก้ไขแล้วในทุกระบบที่ได้รับผลกระทบเมื่อเดือนมีนาคม 2022 ยกเว้นพีซีไคลเอ็นต์และช่องโหว่ CVE-2022-31644, CVE-2022-31645 และ CVE-2022-31646 ได้รับการ อัปเดตความปลอดภัยเมื่อวันที่ 9 สิงหาคม 2022

ที่มาของข่าว : https://www.bleepingcomputer.com/news/security/firmware-bugs-in-many-hp-computer-models-left-unfixed-for-over-a-year/