ประจำวันพฤหัสบดีที่ 11 สิงหาคม 2565

Microsoft แก้ไขช่องโหว่ Zero-day ใน Windows Support Diagnostic Tool (CVE-2022-34713)

Microsoft ได้เผยแพร่การอัปเดตความปลอดภัยเพื่อแก้ไขช่องโหว่ซีโร่เดย์ของ Windows ที่มีความรุนแรงสูง โดยการแก้ไขส่วนหนึ่งของ Patch Tuesday สิงหาคม 2022 ข้อบกพร่องด้านความปลอดภัยนี้คือ CVE-2022-34713 และได้รับการตั้งชื่อว่า DogWalk เกิดจากจุดอ่อนของ path traversal ใน Windows Support Diagnostic Tool (MSDT) ที่ผู้โจมตีสามารถใช้ประโยชน์จากการเรียกใช้โค้ดจากระยะไกลบนระบบที่ถูกบุกรุก พวกเขาสามารถทำได้โดยการเพิ่มไฟล์ปฏิบัติการที่ออกแบบมาเพื่อประสงค์ร้ายกับ Windows Startup เมื่อเป้าหมายเปิดไฟล์ .diagcab ที่ได้รับทางอีเมลหรือดาวน์โหลดจากเว็บ ไฟล์ปฏิบัติการที่ฝังไว้จะถูกดำเนินการโดยอัตโนมัติในครั้งต่อไปที่เหยื่อรีสตาร์ทอุปกรณ์ Windows เพื่อทำงานต่างๆ เช่น ดาวน์โหลดเพย์โหลดมัลแวร์เพิ่มเติม

DogWalk ได้รับการเปิดเผยต่อสาธารณะโดย Imre Rad นักวิจัยด้านความปลอดภัย เมื่อสองปีที่แล้ว ในเดือนมกราคม 2020 หลังจากที่ Microsoft ตอบกลับรายงานของเขาว่าจะไม่ให้มีการแก้ไขใดใดเพราะนี่ไม่ใช่ปัญหาด้านความปลอดภัย อย่างไรก็ตามบั๊กของ Microsoft Support Diagnostics Tool ถูกค้นพบอีกครั้งเมื่อเร็วๆ นี้ และกลับมาได้ รับความสนใจจากสาธารณชน โดยนักวิจัย ด้านความปลอดภัย j00sean

จากข้อมูลของ Microsoft พบว่า DogWalk มีผลกับ Windows ทุกรุ่น รวมถึงเครื่องลูกข่ายและเซิร์ฟเวอร์รุ่นล่าสุด Windows 11 และ Windows Server 2022 โดยเมื่อเดือนที่แล้ว Microsoft เผยแพร่คำแนะนำด้านความปลอดภัยอย่างเป็นทางการ เกี่ยวกับ Windows MSDT Zero-day อื่น (หรือที่เรียกว่า Follina) หลังจากปฏิเสธรายงานเบื้องต้นว่า ไม่ใช่ "ปัญหาที่เกี่ยวข้องกับความปลอดภัย "

วันนี้ บริษัทยังได้เผยแพร่การอัปเดตด้านความปลอดภัยเพื่อจัดการกับ Zero-day ที่เปิดเผยต่อสาธารณะ CVE-2022-30134 - ช่องโหว่การเปิดเผยข้อมูลของ Microsoft Exchange' ซึ่งช่วยให้ผู้โจมตีสามารถอ่านข้อความอีเมลเป้าหมายได้ โดยรวมแล้ว Microsoft ได้แก้ไขช่องโหว่ 112 รายการ ซึ่งเป็นส่วนหนึ่งของ Patch Tuesday ประจำเดือนสิงหาคม 2022 รวมถึงช่องโหว่ที่สำคัญ 17 รายการที่ช่วยให้สามารถเรียกใช้โค้ดจากระยะไกลและยกระดับสิทธิ์ได้

ที่มาของข่าว : https://www.bleepingcomputer.com/news/microsoft/microsoft-patches-windows-dogwalk-zero-day-exploited-in-attacks/