ประจำวันพฤหัสบดีที่ 2 มิถุนายน 2565

ช่องโหว่ Zero-Day "Follina" ใน Microsoft Support Diagnostic Tool (MSDT)

ช่องโหว่ "Follina" ใน Microsoft Support Diagnostic Tool (MSDT) ที่มีผลกับ Windows ทุกรุ่นที่รองรับในปัจจุบันนี้นั้น พบผู้โจมตีกำลังใช้ประโยชน์จากช่องโหว่ที่ไม่ได้รับการแก้ไขและง่ายต่อการใช้ประโยชน์จาก Microsoft Support Diagnostic Tool (MSDT) ใน Windows ที่อนุญาตให้เรียกใช้โค้ดจากระยะไกลจากเอกสาร Office แม้ว่า macros จะถูกปิดใช้งานก็ตาม ซึ่งช่องโหว่นี้มีอยู่ใน Windows ทุกรุ่นและสามารถใช้ประโยชน์ได้ผ่าน Microsoft Office เวอร์ชัน 2013 ถึง Office 2019, Office 2021, Office 365 และ Office ProPlus

โดยผู้โจมตีสามารถใช้ช่องโหว่ Zero-day ที่เรียกว่า "Follina" เพื่อรันโค้ดได้ตามอำเภอใจจากระยะไกลบนระบบ Windows Microsoft ได้เตือนถึงปัญหาที่ทำให้ผู้โจมตีสามารถ "ติดตั้งโปรแกรม ดู เปลี่ยนแปลง หรือลบข้อมูล หรือสร้างบัญชีใหม่ที่อนุญาตโดยสิทธิ์ของผู้ใช้" ทั้งนี้มีนักวิจัยได้รายงานว่าการสังเกตการณ์การโจมตีที่ใช้ประโยชน์จากข้อบกพร่องในอินเดียและรัสเซียจะย้อนกลับไปอย่างน้อยหนึ่งเดือน

โดยมีคำแนะนำจากนักวิจัยให้องค์กรปฏิบัติตามคำแนะนำของ Microsoft กับเครื่องมือวินิจฉัย" แม้ว่าช่องโหว่ใน Mทันที และปิดใช้งานโปรโตคอล MSDT URL "สิ่งนี้จะระงับการเชื่อมโยงระหว่าง OfficeSDT จะยังคงปรากฏอยู่ แต่ก็ไม่สามารถเปิดใช้ได้อีกต่อไปเมื่อเปิดเอกสารที่เป็นอันตราย และให้องค์กรปิดการใช้งานบานหน้าต่างแสดงตัวอย่างใน Windows Explorer ทั้งนี้ Dray Agha นักวิเคราะห์ ThreatOps ที่ Huntress ซึ่งเจาะลึกถึงช่องโหว่ดังกล่าว กล่าวว่าผู้โจมตีสามารถใช้ Follina เพื่อยกระดับสิทธิ์และสามารถสร้างความเสียหายได้ "แฮกเกอร์สามารถเปลี่ยนจากการเป็นผู้ใช้งานทั่วไป กลายไปเป็นผู้ดูแลระบบได้ง่ายมาก"

ที่มาของข่าว : https://www.darkreading.com/endpoint/attackers-actively-exploiting-new-microsoft-zero-day