ประจำวันพฤหัสบดีที่ 11 สิงหาคม 2565

CISA ออกคำเตือนเกี่ยวกับการใช้ประโยชน์จากซอฟต์แวร์ UnRAR สำหรับระบบ Linux

เมื่อวันอังคารที่ผ่านมาสำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐอเมริกา (CISA) ได้เพิ่มรายการช่องโหว่ด้านความปลอดภัยที่เพิ่งถูกเปิดเผยในยูทิลิตี้ UnRAR ลงในแค็ตตาล็อกช่องโหว่ที่รู้จักซึ่งอ้างอิงจากหลักฐานที่บ่งชี้ว่ามีการแสวงหาประโยชน์ที่ใช้งานอยู่ ที่หมายเลขช่องโหว่ CVE-2022-30333 (คะแนน CVSS : 7.5) เป็นช่องโหว่การข้ามเส้นทางใน UnRAR เวอร์ชัน Unix ที่สามารถทริกเกอร์ได้เมื่อแยกไฟล์เก็บถาวร RAR ซึ่งช่องโหว่นี้ถูกออกแบบเพื่อประสงค์ร้ายซึ่งผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่เพื่อวางไฟล์ตามอำเภอใจบนระบบเป้าหมายที่มีการติดตั้งยูทิลิตี้เพียงแค่ decompressed file

ช่องโหว่ดังกล่าวถูกเปิดเผยโดย Simon Scannell นักวิจัย SonarSource เมื่อปลายเดือนมิถุนายน โดย RARLAB UnRAR บน Linux และ UNIX มีช่องโหว่การข้ามผ่านไดเร็กทอรีซึ่งช่วยให้ผู้โจมตีสามารถเขียนไปยังไฟล์ระหว่างการดำเนินการแยก จึงไม่ค่อยมีใครรู้เกี่ยวกับการโจมตี แต่เมื่อการเปิดเผยนี้อาจทำให้แนวโน้มการโจมตีเพิ่มขึ้นซึ่งผู้โจมตีสามารถสแกนหาระบบที่มีช่องโหว่ได้อย่างรวดเร็วหลังจากมีการเปิดเผยช่องโหว่ต่อสาธารณะและใช้โอกาสในการปล่อยมัลแวร์และแคมเปญแรนซัมแวร์

กล่าวกันว่าเป็นช่องโหว่รูปแบบหนึ่งที่รู้จักกันทั่วไปในชื่อ DogWalk ช่องโหว่ในคอมโพเนนต์ Microsoft Windows Support Diagnostic Tool (MSDT) อาจใช้โดยผู้โจมตีสามารถรันโค้ดตามอำเภอใจบนระบบที่มีช่องโหว่ โดยหลอกให้เปิดไฟล์ ซึ่งหน่วยงานของรัฐบาลกลางในสหรัฐอเมริกาได้รับคำสั่งให้มีการอัปเดตช่องโหว่ภายในวันที่ 30 สิงหาคม เพื่อลดความเสี่ยงต่อการถูกโจมตีทางไซเบอร์

ที่มาของข่าว : https://thehackernews.com/2022/08/cisa-issues-warning-on-active.html