ประจำวันอังคารที่ 28 มิถุนายน 2565

Log4Shell ยังคงถูกแฮ็กเซิร์ฟเวอร์ VMWare เพื่อกรองข้อมูลที่ละเอียดอ่อน

สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐฯ (CISA) พร้อมด้วยหน่วยบัญชาการทางไซเบอร์ของหน่วยยามฝั่ง (CGCYBER) ออกคำเตือนร่วมกันเกี่ยวกับความพยายามอย่างต่อเนื่องในส่วนของผู้โจมตีที่ใช้ประโยชน์จากช่องโหว่ Log4Shell ในเซิร์ฟเวอร์ VMware Horizon เพื่อโจมตีเป้าหมายเครือข่าย ตั้งแต่ธันวาคม 2564 กลุ่มผู้ก่อภัยคุกคามหลายกลุ่มได้ใช้ประโยชน์จาก Log4Shell บนเซิร์ฟเวอร์ VMware Horizon ที่ไม่มีการแพตช์และเปิดสู่สาธารณะ ส่วนหนึ่งของการโจมตีนี้ ทำให้ผู้โจมตี APT ได้ฝังมัลแวร์ไว้บนระบบที่ถูกโจมตีด้วยโปรแกรมสั่งการที่ฝังตัวซึ่งจะเปิดใช้งานคำสั่งและการควบคุมจากระยะไกล (C2)

Log4Shell ที่หมายเลขช่องโหว่ CVE-2021-44228 (คะแนน CVSS : 10.0) เป็นช่องโหว่ในการเรียกใช้โค้ดจากระยะไกลที่ส่งผลต่อไลบรารีการบันทึก Apache Log4j ที่ใช้โดยผู้ใช้งานและบริการระดับองค์กร เว็บไซต์ แอปพลิเคชัน และผลิตภัณฑ์อื่นๆ ที่หลากหลาย การใช้ประโยชน์จากช่องโหว่ที่สำเร็จอาจทำให้ผู้โจมตีสามารถส่งคำสั่งที่ออกแบบมาเป็นพิเศษไปยังระบบที่ได้รับผลกระทบ ทำให้ผู้โจมตีสามารถรันโค้ดที่เป็นอันตรายและเข้าควบคุมเป้าหมายได้

โดยกิจกรรมที่เกี่ยวข้องกับ Log4Shell ยังคงมีดำเนินการอยู่แม้ว่าจะผ่านมานานกว่าหกเดือนแล้ว ซึ่งแสดงให้เห็นว่าช่องโหว่ดังกล่าวเป็นที่สนใจของผู้โจมตี ซึ่งรวมถึงภัยคุกคามขั้นสูงแบบต่อเนื่อง (APT) ที่ได้รับการสนับสนุนจากรัฐ ซึ่งได้กำหนดเป้าหมายไปยังเซิร์ฟเวอร์ที่ไม่ได้รับการแพตช์โดยฉวยโอกาสในการโจมตีในเบื้องต้น

จากข้อมูลของบริษัทความปลอดภัยทางไซเบอร์ ExtraHop ช่องโหว่ของ Log4j นั้นได้รับความพยายามในการสแกนอย่างไม่หยุดยั้ง โดยภาคการเงินและสุขภาพกลายเป็นตลาดที่มีขนาดใหญ่สำหรับการโจมตีที่อาจเกิดขึ้น

ที่มาของข่าว : https://thehackernews.com/2022/06/log4shell-still-being-exploited-to-hack.html