แฮ็กเกอร์ชาวอิหร่าน เจาะช่องโหว่ VMware เพื่อติดตั้งแบ็กดอร์ “Core Impact”

แฮ็กเกอร์ที่มีส่วนเกี่ยวข้องกับทางอิหร่านที่รู้จักกันในชื่อ Rocket Kitten ได้เจาะช่องโหว่บน VMware ที่มีการออกแพ็ตช์แล้ว เพื่อเข้าถึงระบบภายในของเหยื่อ แล้วติดตั้งทูลทดสอบเจาะระบบที่ชื่อ Core Impact โดยช่องโหว่นี้อยู่ภายใต้รหัส CVE-2022-22954 (CVSS score: 9.8)

ช่องโหว่นี้เปิดให้รันโค้ดได้จากระยะไกล (RCE) กระทบกับ VMware Workspace ONE Access and Identity Manager ซึ่งมีการออกแพ็ตช์มาแล้วเมื่อวันที่ 6 เมษายนที่ผ่านมา พร้อมทั้งแจ้งเตือนผู้ใช้หลังพบการใช้ประโยชน์จากช่องโหว่นี้ในวงกว้างให้หลังหนึ่งสัปดาห์ด้วย

นักวิจัยจาก Morphisec Labs กล่าวในรายงานว่า ผู้ที่ใช้ช่องโหว่ RCE นี้จะสามารถใช้โจมตีต่อได้แบบไร้ขีดจำกัด เนื่องจากได้การเข้าถึงในระดับสิทธิ์ที่สูงที่สุดไม่ว่าจะเป็นส่วนไหนของโฮสต์เวอร์ช่วล หรือแม้แต่ระบบเกสก็ตาม

กลไกการโจมตีผ่านช่องโหว่นี้มีการใช้สเตเจอร์บนพาวเวอร์เชลล์เพื่อดาวน์โหลดข้อมูลอันตรายลำดับถัดมาที่ชื่อ PowerTrash Loader จากนั้นก็จะใช้ฝังทูลทดสอบการเจาะระบบ Core Impact ในหน่วยความจำที่คอยตรวจสอบความเคลื่อนไหวของเหยื่อ

ที่มา THN