ประจำวันพฤหัสบดีที่ 4 สิงหาคม 2565

VMware ออกแพตช์สำหรับแก้ไขข้อบกพร่องใหม่ที่ส่งผลต่อผลิตภัณฑ์หลายรายการ

VMware ผู้ให้บริการ Virtualization ได้ออกแพตช์การอัปเดตเพื่อแก้ไขข้อบกพร่องด้านความปลอดภัย 10 ข้อ ที่ส่งผลต่อผลิตภัณฑ์หลายรายการที่อาจนำไปใช้ในทางที่ผิด โดยผู้โจมตีไม่ต้องผ่านการตรวจสอบสิทธิ์เพื่อดำเนินการที่เป็นอันตรายได้

โดยหมายเลข CVE ตั้งแต่ CVE-2022-31656 ถึง CVE-2022-31665 (คะแนน CVSS: 4.7 - 9.8) ส่งผลต่อ VMware Workspace ONE Access, Workspace ONE Access Connector, Identity Manager, Identity Manager Connector, vRealize Automation, Cloud Foundation และ vRealize โดยข้อบกพร่องที่ร้ายแรงที่สุดคือ CVE-2022-31656 (คะแนน CVSS: 9.8) ซึ่งเป็นช่องโหว่ข้ามการตรวจสอบสิทธิ์ที่ส่งผลต่อผู้ใช้โดเมนในเครื่องที่ผู้ไม่หวังดี ที่มีการเข้าถึงเครือข่ายสามารถใช้ประโยชน์จากการเข้าถึงระดับผู้ดูแลระบบได้ นอกจากนี้ VMware ยังได้แก้ไขช่องโหว่การเรียกใช้โค้ดจากระยะไกล จำนวน 3ช่องโหว่ (CVE-2022-31658, CVE-2022-31659 และ CVE-2022-31665) ที่เกี่ยวข้องกับ JDBC และ SQL injection

โดย VMware ได้แนะนำให้ลูกค้าที่ใช้ผลิตภัณฑ์ที่มีช่องโหว่ ทำการแพตช์ในทันทีเพื่อบรรเทาภัยคุกคามที่อาจเกิดขึ้น

ที่มาของข่าว : https://thehackernews.com/2022/08/vmware-releases-patches-for-several-new.html