ประจำวันพฤหัสบดีที่ 16 มิถุนายน 2565

ช่องโหว่ใหม่ของอีเมล Zimbra อาจทำให้ผู้โจมตีขโมยข้อมูลที่ใช้รับรองการเข้าสู่ระบบ

ช่องโหว่ใหม่ที่มีความรุนแรงสูงได้รับการเปิดเผยในอีเมลของ Zimbra หากถูกโจมตีสำเร็จจะทำให้ผู้โจมตีที่ไม่ผ่านการตรวจสอบสิทธิ์สามารถขโมยรหัสผ่านแบบข้อความธรรมดาของผู้ใช้งานได้ และเมื่อเข้าถึงกล่องจดหมายของผู้ใช้งาน จะทำให้ผู้โจมตีสามารถเพิ่มการเข้าถึงองค์กรและเข้าถึงบริการภายในต่างๆ และขโมยข้อมูลที่มีความละเอียดอ่อนสูง

โดยหมายเลขช่องโหว่ CVE-2022-27924 (คะแนน CVSS : 7.5) ปัญหานี้เกิดจาก Memcached กับคำขอที่ไม่ผ่านการตรวจสอบสิทธิ์ ซึ่งอาจนำไปสู่สถานการณ์ที่ฝ่ายผู้โจมตีสามารถแทรกคำสั่งที่เป็นอันตรายและดูดข้อมูลที่มีความละเอียดอ่อนได้เนื่องจาก Memcached แยกวิเคราะห์คำขอที่เข้ามาทีละบรรทัด ทำให้ช่องโหว่นี้อนุญาตให้ผู้โจมตีส่งคำขอค้นหาที่สร้างขึ้นเป็นพิเศษไปยังเซิร์ฟเวอร์ที่มีอักขระ CRLF ทำให้เซิร์ฟเวอร์ดำเนินการคำสั่งที่ไม่ได้ตั้งใจ

โดยนักวิจัยกล่าวว่าช่องโหว่ของโค้ดนี้ทำให้ผู้โจมตีสามารถขโมยข้อมูลหรือการรับรองข้อความจากผู้ใช้อินสแตนซ์ Zimbra ที่เป็นเป้าหมายได้ จากความสามารถนี้ ผู้โจมตีจะสามารถทำให้แคชเสียหายในภายหลังเพื่อทำการเขียนทับรายการ โดยส่งต่อการรับส่งข้อมูล IMAP ทั้งหมดไปยังเซิร์ฟเวอร์ที่ควบคุมโดยผู้โจมตี รวมถึงข้อมูลรับรองของผู้ใช้ที่เป็นเป้าหมายในข้อความธรรมดา เมื่อได้ครอบครองที่อยู่อีเมลของผู้ใช้งานจะสามารถวางรายการแคชและใช้ไคลเอ็นต์ IMAP เพื่อดึงข้อความอีเมลจากเซิร์ฟเวอร์อีเมล

หลังจากเปิดเผยข้อมูลเมื่อวันที่ 11 มีนาคม 2022 จึงมีการออกแพตช์เพื่ออุดช่องโหว่ด้านความปลอดภัยทั้งหมดโดย Zimbra เมื่อวันที่ 10 พฤษภาคม 2022 ในเวอร์ชัน 8.8.15 P31.1 และ 9.0.0 P24.1

ที่มาของข่าว : https://thehackernews.com/2022/06/new-zimbra-email-vulnerability-could.html