แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

บริษัทผู้พัฒนาผลิตภัณฑ์ Veeam Backup & Replication ออกอัปเดตด้านความมั่นคงปลอดภัยแก้ไขช่องโหว่หลายรายการ

วันที่แจ้งเตือน 13 มีนาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า บริษัท Veeam ได้เปิดเผยเกี่ยวกับช่องโหว่หลายรายการในผลิตภัณฑ์ Veeam Backup & Replication (VBR) ซึ่งผู้ไม่หวังดีสามารถโจมตีแบบ Remote Code Execution (RCE) ได้

ช่องโหว่ที่เกี่ยวข้องได้แก่ CVE-2026-21666, CVE-2026-21667 และ CVE-2026-21669 ซึ่งกระทบต่อ VBR เวอร์ชัน 12.3.2.4165 และก่อนเวอร์ชัน 12 ทั้งหมด โดยผู้ไม่หวังดีสามารถรันโค้ดหรือเขียนไฟล์ในระบบด้วยสิทธิ์ระดับสูง เช่น root หรือสิทธิ์ของบัญชีผู้ดูแลฐานข้อมูล เป็นต้น และเข้าควบคุมเซิร์ฟเวอร์สำรองข้อมูลและข้อมูลสำคัญขององค์กรได้ และช่องโหว่ CVE-2026-21708 ส่งผลกระทบ VBR เวอร์ชัน 13.0.1.180 และก่อนเวอร์ชัน 13 โดยผู้ไม่หวังดีใช้ช่องโหว่นี้เพื่อยกระดับสิทธิ์เป็น Backup Operator หรือ Tape Operator ส่งคำสั่งอันตรายและรันโค้ดในสิทธิ์ของผู้ใช้ postgres เพื่อโจมตีระบบ

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบตรวจสอบการใช้งานซอฟต์แวร์ Veeam Backup & Replication และดำเนินการอัปเดตซอฟต์แวร์เป็นเวอร์ชันล่าสุดที่ได้รับคำแนะนำจากผู้ผลิต พร้อมทั้งทบทวนการกำหนดสิทธิ์ผู้ใช้งานที่มีสิทธิ์ระดับสูงในระบบ นอกจากนี้ควรดำเนินการเฝ้าระวังบันทึกเหตุการณ์ (Log Monitoring) และกิจกรรมที่ผิดปกติในระบบสำรองข้อมูล เพื่อให้สามารถตรวจจับและตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ได้อย่างทันท่วงที

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://www.bleepingcomputer.com/news/security/veeam-warns-of-critical-flaws-exposing-backup-servers-to-rce-attacks/
2. https://nvd.nist.gov/vuln/detail/CVE-2026-21666
3. https://nvd.nist.gov/vuln/detail/CVE-2026-21667
4. https://nvd.nist.gov/vuln/detail/CVE-2026-21669
5. https://nvd.nist.gov/vuln/detail/CVE-2026-21708