แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ร้ายแรงของผลิตภัณฑ์ Veeam Backup & Replication (CVE-2025-23120)

วันที่แจ้งเตือน 27 มีนาคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงของผลิตภัณฑ์ Veeam Backup & Replication (CVE-2025-23120) โดยช่องโหว่ดังกล่าวเป็นช่องโหว่ Deserialization ซึ่งจะเกิดขึ้นเมื่อแอปพลิเคชันประมวลผลข้อมูลที่ถูกตรวจสอบอย่างไม่เหมาะสม ทำให้ผู้ไม่หวังดีสามารถแทรก objects หรือ gadgets เพื่อเรียกใช้โค้ดที่เป็นอันตรายจากระยะไกล (Remote Code Execution) บนเซิร์ฟเวอร์ได้ ทั้งนี้ ส่งผลกระทบเฉพาะกับการติดตั้ง Veeam Backup & Replication ที่เชื่อมต่อกับ Domain controller เท่านั้น ซึ่งอาจทำให้ผู้ใช้งานทุกคนในโดเมนสามารถใช้ช่องโหว่นี้ในการเข้าถึง Backup Server ได้

Veeam ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเดตซอฟต์แวร์ Veeam Backup & Replication เป็นเวอร์ชันตามที่แนะนำโดยเร็วที่สุด

Product Name	Affected Version	Solution
Veeam Backup & Replication	12.3.0.310 และ เวอร์ชัน 12 รุ่นก่อนหน้าทั้งหมด	Upgrade to 12.3.1

ThaiCERT แนะนำให้หน่วยงานควรเฝ้าระวังและตรวจสอบช่องโหว่ภายในบริษัทและตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของบริษัทเป็นประจำสม่ำเสมอ

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสมเพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 27 มี.ค. 2568
2) https://www.veeam.com/kb4724
3) https://nvd.nist.gov/vuln/detail/CVE-2025-23120