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

แจ้งเตือนช่องโหว่ร้ายแรงของผลิตภัณฑ์ Veeam Recovery Orchestrator (CVE-2024-29855)

วันที่แจ้งเตือน 13 มิถุนายน 2567

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

บริษัท Veeam* ได้เผยแพร่รายการช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Veeam Recovery Orchestrator (VRO) (CVE-2024-29855) โดยช่องโหว่ดังกล่าวเกิดจากการ Hard-coded JWT (JSON Web Token) บน VRO ซึ่งทำให้ผู้ไม่หวังดีสามารถข้ามขั้นตอนการพิสูจน์ตัวตน (authentication bypass) และสามารถเข้าถึง VRO web UI ด้วยสิทธิผู้ดูแลระบบได้ (administrative privileges)

ทั้งนี้ Veeam ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเกรดซอฟต์แวร์เป็นเวอร์ชันตามที่แนะนำ หรือ ติดตั้งแพตช์โดยเร็วที่สุดดังตาราง

Product	Affected	Solution
Veeam Recovery Orchestrator	VRO 7.0.0.337	อัปเกรดเป็น เวอร์ชัน 7.1.0.230 หรือ ติดตั้ง patch update เป็น build 7.0.0.379
	VRO 7.1.0.205	ติดตั้ง patch update เป็น build 7.1.0.230

อย่างไรก็ดี ช่องโหว่ดังกล่าวไม่กระทบกับผลิตภัณฑ์อื่น ๆ ของ Veeam เช่น Veeam Backup & Replication, Veeam Agent for Microsoft Windows, Veeam ONE และ Veeam Service Provider Console

ก.ล.ต. เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นกับการปฏิบัติงานของบริษัท

* Veeam บริษัทผู้ให้บริการซอฟต์แวร์และโซลูชัน การสำรองข้อมูล และการกู้คืนข้อมูลภายในองค์กร

ข้อมูลอ้างอิง

https://www.veeam.com/kb4585