แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ SQL injection ใน Cacti

วันที่แจ้งเตือน 8 กรกฎาคม 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้เผยแพร่รายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ กรณีช่องโหว่ SQL injection ใน Cacti โดยมีรายละเอียดดังนี้

การโจมตี	ผลิตภัณฑ์หรือระบบที่อาจได้รับผลกระทบ
ช่องโหว่ CVE-2026-39955 Improper Neutralization of Special Elements used in an SQL Command หรือ SQL Injection ใน Cacti ซึ่งเป็นซอฟต์แวร์ Open Source สำหรับบริหารจัดการและติดตามประสิทธิภาพเครือข่าย โดยช่องโหว่นี้เป็นการโจมตีแบบ Pre-Authentication SQL Injection ในไฟล์ graph_view.php จากการตรวจสอบค่า FILTER_VALIDATE_REGEXP ที่ไม่ปลอดภัย ส่งผลให้ผู้ไม่หวังดีสามารถแทรกคำสั่ง SQL เข้าถึงและแก้ไขข้อมูลในฐานข้อมูลของระบบได้ **ผู้ไม่หวังดีเข้าหน้าเว็บ Cacti –> ส่งคำสั่ง SQL แฝงเข้ามา –> ระบบตรวจสอบไม่รัดกุม –> ฐานข้อมูลถูกสั่งงานโดยไม่ได้รับอนุญาต –> ข้อมูลรั่วไหล หรือระบบถูกยึด**	Cacti เวอร์ชัน 1.2.30 และก่อนหน้า **ผู้ไม่หวังดีสามารถเข้าควบคุมระบบได้โดยไม่ต้อง Login และอาจใช้เป็นจุดเริ่มต้นโจมตีระบบอื่นต่อ**

แนวทางการป้องกันและลดความเสี่ยง

- อัปเดต Cacti เป็นเวอร์ชัน 1.2.31 หรือเวอร์ชันที่ได้รับการแก้ไขจากผู้ผลิตโดยเร็วที่สุด
- จำกัดการเข้าถึง Cacti Web Interface ให้เข้าถึงเฉพาะเครือข่ายภายในหรือ IP Address ที่เชื่อถือได้
- หลีกเลี่ยงการเปิดระบบ Cacti ให้เข้าถึงจากอินเทอร์เน็ตโดยตรง
- ทำ input validation และใช้หลัก least privilege เพื่อลดผลกระทบ
- เฝ้าระวัง Log การใช้งานที่ผิดปกติ โดยเฉพาะคำขอที่เกี่ยวข้องกับ graph_view.php หรือพารามิเตอร์ที่มีลักษณะเป็น SQL Injection

ข้อมูลอ้างอิง

1. รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 7 ก.ค. 2569
2. https://nvd.nist.gov/vuln/detail/CVE-2026-39955?
3. https://www.ionix.io/threat-center/cve-2026-39955/?

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ