แจ้งเตือน : ช่องโหว่

Critical

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

แจ้งเตือน กลุ่ม Cactus Ransomware ใช้ประโยชน์จากช่องโหว่ร้ายแรงในผลิตภัณฑ์ Qlik Sense Enterprise for Windows

วันที่แจ้งเตือน 7 พฤษภาคม 2567

สืบเนื่องจาก ThaiCERT สกมช. ได้เผยแพร่รายงานพบกลุ่มผู้ไม่หวังดี Cactus Ransomware ว่ามีการใช้ประโยชน์จากช่องโหว่ที่มีผลกระทบร้ายแรงในซอฟต์แวร์ Qlik Sense Enterprise for Windows (CVE-2023-41265, CVE-2023-41266 และ CVE-2023-48365) และสำนักงานได้นำส่งข่าวแจ้งเตือนดังกล่าวให้แก่ผู้ประกอบธุรกิจทราบ เมื่อวันที่ 22 มีนาคม 2567 แล้วนั้น

ปัจจุบันนักวิจัยจากบริษัทรักษาความปลอดภัยทางไซเบอร์ ได้รายงานตัวบ่งชี้ภัยคุกคาม (Indicator of Compromise : IoCs) ที่กลุ่มผู้ไม่หวังดีใช้ในการโจมตีเพิ่มเติม โดยมีรายละเอียดตาม **เอกสารแนบ**

ผู้ประกอบธุรกิจควรพิจารณาอัปเดตเวอร์ชันของซอฟต์แวร์ตามที่ Qlik* แนะนำ โดยควรประเมินความเสี่ยง และดำเนินการทดสอบก่อนนำไปใช้งานจริง พร้อมทั้งจัดให้มีมาตรการควบคุมอย่างเหมาะสม เพื่อป้องกันผลกระทบที่อาจเกิดขึ้น

หมายเหตุ* บริษัทผู้พัฒนาซอฟต์แวร์ที่ช่วยในการสรุปภาพรวมของข้อมูลในหลายมิติ (Data Visualization) เพื่อสะท้อนผลการดำเนินงาน สนับสนุนทางเลือกในการตัดสินใจ และช่วยในการวางแผน

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 7 พ.ค. 2567
2) https://community.qlik.com/t5/Official-Support-Articles/Critical-Security-fixes-for-Qlik-Sense-Enterprise-for-Windows/Ta-p/2110801
3) https://www.bleepingcomputer.com/news/security/cactus-ransomware-exploiting-qlik-sense-flaws-to-breach-networks/