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 กลุ่ม Cactus Ransomware ใช้ประโยชน์จากช่องโหว่ร้ายแรง ในผลิตภัณฑ์ Qlik Sense Enterprise for Windows

วันที่แจ้งเตือน 22 มีนาคม 2567

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ได้เผยแพร่รายงานพบกลุ่มผู้ไม่หวังดี Cactus Ransomware ว่ามีการใช้ประโยชน์จากช่องโหว่ที่มีผลกระทบร้ายแรงในซอฟต์แวร์ Qlik Sense Enterprise for Windows (CVE-2023-41265, CVE-2023-41266 และ CVE-2023-48365) ซึ่งส่งผลให้ผู้ไม่หวังดีสามารถเข้าถึงเครื่องแม่ข่ายที่ติดตั้งซอฟต์แวร์ดังกล่าวได้โดยไม่ได้รับอนุญาต รวมถึงสามารถส่งคำสั่งจากระยะไกลได้โดยไม่ต้องผ่านการพิสูจน์ตัวตน (Remote Code Execution : RCE) ได้

ทั้งนี้ เวอร์ชันซอฟต์แวร์ที่ได้รับผลกระทบ ได้แก่ Qlik Sense Enterprise for Windows เวอร์ชันก่อนหน้ารวมถึงเวอร์ชันดังนี้

- May 2023 Patch 3
- February 2023 Patch 7
- November 2022 Patch 10
- August 2022 Patch 12

ดังนั้น Qlik จึงแนะนำให้อัปเดตเวอร์ชัน เพื่อแก้ไขช่องโหว่ดังนี้

- August 2023 Patch 2
- May 2023 Patch 6
- February 2023 Patch 10
- November 2022 Patch 12
- August 2022 Patch 14
- May 2022 Patch 16
- February 2022 Patch 15
- November 2021 Patch 17

นอกจากนี้นักวิจัยจากบริษัทรักษาความปลอดภัยทางไซเบอร์ ได้รายงานตัวบ่งชี้ภัยคุกคาม (Indicator of Compromise : IoCs) ที่กลุ่มผู้ไม่หวังดีใช้ในการโจมตี โดยมีรายละเอียดตาม**เอกสารแนบ** ผู้ประกอบธุรกิจควรพิจารณาอัปเดตเวอร์ชันของซอฟต์แวร์ตามที่ Qlik Sense แนะนำ โดยควรประเมินความเสี่ยง และดำเนินการทดสอบก่อนนำไปใช้งานจริง พร้อมทั้งจัดให้มีมาตรการควบคุมอย่างเหมาะสมเพื่อป้องกันผลกระทบที่อาจเกิดขึ้น

หมายเหตุ* บริษัทผู้พัฒนาซอฟต์แวร์ที่ช่วยในการสรุปภาพรวมของข้อมูลในหลายมิติ เพื่อสะท้อนผลการดำเนินงาน สนับสนุนทางเลือกในการตัดสินใจ และช่วยในการวางแผน

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 21 มี.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/