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

CISA และ FBI ออกคำแนะนำการกู้คืน ESXiArgs Ransomware

วันที่แจ้งเตือน 15 กุมภาพันธ์ 2566

ตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ และ ก.ล.ต. ได้แจ้งเตือนเกี่ยวกับการโจมตีด้วย Ransomware จำนวนมาก โดยใช้ช่องโหว่บน VMware ESXi (CVE-2021-21974) เมื่อวันที่ 8 ก.พ. 2566 นั้น คลิกอ่านได้ที่ https://www.sec.or.th/TH/Documents/CyberResilience/cyber-alert-36.pdf

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ได้แจ้งคำแนะนำของ Cybersecurity and Infrastructure Security Agency (CISA) และสำนักงานสืบสวนกลางแห่งสหรัฐอเมริกา (FBI) เกี่ยวกับความปลอดภัยทางไซเบอร์ (Cybersecurity Advisory: CSA) เพื่อตอบสนองต่อ Ransomware campaign ที่กำลังแพร่ระบาดอยู่ขณะนี้ ชื่อว่า “ESXiArgs” โดยผู้ไม่หวังดีใช้ประโยชน์จากช่องโหว่บนซอฟต์แวร์เครื่องแมขาย VMware ESXi ที่ไม่ได้รับการติดตั้งชุดอัปเดตซอฟต์แวร์ (Patch) และใช้งานเวอร์ชันล้าสมัย เพื่อเข้าถึงระบบ และติดตั้งใช้งาน Ransomware “ESXiArgs” และเข้ารหัสไฟล์การตั้งค่า (Configuration file) บนเครื่องแม่ข่าย Vmware ESXi ซึ่งอาจทำให้เครื่องแม่ข่ายไม่สามารถให้บริการได้

โดย CISA และ FBI สนับสนุนให้ทุกองค์กรที่มีการใช้งาน VMware ESXi ดำเนินการดังนี้:

- อัปเดตซอฟต์แวร์ VMware ESXi ให้เป็นเวอร์ชันล่าสุด
- ปิดการใช้งานบริการ Service Location Protocol (SLP) และ
- ไม่เชื่อมต่อ ESXi กับอินเทอร์เน็ตสาธารณะ

อย่างไรก็ดี หากองค์กรได้รับผลกระทบจาก Ransomware “ESXiArgs” ทาง CISA และ FBI แนะนำให้ปฏิบัติตามคำแนะนำ[3] (Guidance) และ สคริปต์การกู้คืน[4] (Recovery script) ที่ระบุไว้ใน CSA ในการดำเนินการกู้คืน

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ใช้งานและผู้ดูแลระบบ ควรพิจารณาดำเนินการอัปเดต ESXi เป็นเวอร์ชันล่าสุดทันที และปฏิบัติตามที่ CISA และ FBI แนะนำ โดยผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันพฤหัสบดีที่ 9 กุมภาพันธ์ 2566
2) https://www.cisa.gov/uscert/ncas/alerts/aa23-039a
3) https://www.cisa.gov/uscert/ncas/current-activity/2023/02/08/cisa-and-fbi-release-esxiargs-ransomware-recovery-guidance
4) https://github.com/cisagov/ESXiArgs-Recover