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

แจ้งเตือนการโจมตีด้วย Ransomware แบบมุ่งเป้า โดยใช้ช่องโหว่บน VMware ESXi (CVE-2021-21974)

วันที่แจ้งเตือน 12 ธันวาคม 2566

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT)[1] หรือ สกมช. ได้เผยแพร่รายงานเกี่ยวกับ Ransomware Campaign โดยบริษัท VMware และหน่วยงานรัฐบาลในกลุ่มประเทศยุโรป ที่แจ้งเตือนผู้ใช้งาน VMware ESXi Hypervisor ถึงการระบาดของ ransomware ใน ESXi ที่ยังไม่ได้รับการติดตั้งซอฟต์แวร์แก้ไขช่องโหว่ (patch) โดยกลุ่มผู้ไม่หวังดีจะโจมตีผ่านช่องโหว่ CVE-2021-21974 ทำให้หน่วยความจำของระบบเกิดการล้นของข้อมูล (heap-overflow) ในบริการ OpenSLP (Service Location Protocol) ผ่านพอร์ต 427 (TCP/UDP) บน ESXi ซึ่งช่องโหว่นี้ได้ออก patch ล่าสุดเมื่อปี 2021 ทั้งนี้ หากการโจมตีสำเร็จจะส่งผลให้ผู้โจมตีสามารถเข้าถึงระบบโดยไม่ต้องผ่านการยืนยันตัวตนได้ โดยเวอร์ชันที่ได้รับผลกระทบมีดังต่อไปนี้

- ESXi เวอร์ชัน 7.x ก่อนหน้า ESXi70U1c-17325551
- ESXi เวอร์ชัน 6.7.x ก่อนหน้า ESXi670-202102401-SG
- ESXi เวอร์ชัน 6.5.x ก่อนหน้า ESXi650-202102101-SG

ทั้งนี้ ThaiCERT แนะนำให้ผู้ใช้งานและผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบดำเนินการลดความเสี่ยงตามคำแนะนำดังนี้

- อัปเดต patch ล่าสุดสำหรับ VMware ESXi และซอฟต์แวร์ที่เกี่ยวข้องทั้งหมด
- ตรวจสอบการตั้งค่าความปลอดภัย โดยปรับแต่งการตั้งค่าความปลอดภัยของระบบ ESXi เพื่อลดความเสี่ยง รวมถึงการปิดการใช้งานบริการหรือพอร์ตที่ไม่จำเป็น
- ตรวจสอบการเข้าถึง และจำกัดการเข้าถึงพอร์ต 427 (TCP/UDP) ที่เกี่ยวข้องกับช่องโหว่ เพื่อลดความเสี่ยงถูกโจมตี
- ตรวจสอบ Log ของระบบเพื่อตรวจพบกิจกรรมที่ผิดปกติ และดำเนินการตอบสนอง
- ตรวจสอบระบบการจัดเก็บข้อมูล เพื่อให้มั่นใจว่ามีข้อมูลสำรองที่ทันสมัย
- พิจารณาการแยกเครือข่าย หรือ การให้การเข้าถึงที่จำกัด เพื่อลดความเสี่ยงของการแพร่กระจายในเครือข่าย
- การฝึกอบรมและการทราบความเสี่ยง ที่เกี่ยวข้องกับการใช้งานและดูแลรักษาระบบ ESXi

เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ใช้งานและผู้ดูแลระบบ ควรพิจารณาดำเนินการอัปเดต ESXi เป็นเวอร์ชันล่าสุดทันทีตามที่ ThaiCERT แนะนำ โดยผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง ทั้งนี้สามารถพิจารณาข้อมูลเพิ่มเติมได้ที่ https://www.forescout.com/blog/vmware-esxi-servers-a-major-attack-vector-for-ransomware/

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันอาทิตย์ที่ 10 ธันวาคม 2566
2) https://www.vmware.com/security/advisories/VMSA-2021-0002.html
3) https://www.csa.gov.sg/singcert/Advisories/ad-2021-009/
4) https://www.forescout.com/blog/vmware-esxi-servers-a-major-attack-vector-for-ransomware/