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 การโจมตีด้วย Ransomware จำนวนมาก โดยใช้ช่องโหว่บน VMware ESXi (CVE-2021-21974)

วันที่แจ้งเตือน 8 กุมภาพันธ์ 2566

Singapore Computer Emergency Response Team (SingCERT) และ สกมช. เผยแพร่รายงานเกี่ยวกับ Ransomware Campaign ที่มีการใช้ประโยชน์จากช่องโหว่เก่าหมายเลข (CVE-2021-21974) บนซอฟต์แวร์เครื่องแม่ข่าย VMware ESXi โดยผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่ดังกล่าวเพื่อโจมตีในรูปแบบการควบคุมระบบจากระยะไกล (Remote code execution) จากการทำให้เกิดการล้นของข้อมูลในหน่วยความจำของระบบ (heap-overflow) ในบริการ OpenSLP (Service Location Protocol) ส่งผลให้สามารถโจมตีระบบโดยไม่ต้องผ่านการยืนยันตัวตน และ เข้าถึงระบบด้วยสิทธิสูงได้ โดยมีเวอร์ชันที่ได้รับผลกระทบดังต่อไปนี้

- 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

ผู้ใช้งานและผู้ดูแลระบบ ที่มีการใช้งาน ESXi เวอร์ชันที่ได้รับผลกระทบ ควรรีบอัปเดตให้เป็นเวอร์ชันล่าสุดทันที เพื่อเป็นการป้องกันจากการถูกโจมตี และ ขอให้ตรวจสอบระบบทั้งหมดเพื่อสแกนหาสัญญาณของการบุกรุก รวมถึง ผู้ใช้งานและผู้ดูแลระบบควรพิจารณาปิดการใช้งานพอร์ต 427(TCP/UDP) บนระบบ ESXi เนื่องจากเป็นพอร์ตที่เป็นเป้าหมายของการโจมตีใน Ransomware Campaign นี้ (พิจารณาผลกระทบก่อนดำเนินการปิดพอร์ตดังกล่าว) และพิจารณาการตั้งค่ากฎบนอุปกรณ์ Firewall เพื่อหยุดการเชื่อมต่อกับ IP address ดังต่อไปนี้

- 104.152.52[.]55
- 193.163.125[.]138
- 43.130.10[.]173
- 104.152.52[.]0/24

ทั้งนี้ SingCERT แนะนำให้ผู้ใช้งานและผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบควรอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ใช้งานและผู้ดูแลระบบควรพิจารณาดำเนินการอัปเดต ESXi เป็นเวอร์ชันล่าสุดทันที ตามที่ SingCERT แนะนำโดยผู้ดูแลระบบควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันจันทร์ที่ 6 กุมภาพันธ์ 2566
2) https://www.csa.gov.sg/en/singcert/Alerts/AL-2023-015
3) https://www.vmware.com/security/advisories/VMSA-2021-0002.html
4) https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/
5) https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/
6) https://www.csa.gov.sg/singcert/Advisories/ad-2021-009/