เรื่อง แจ้งเตือนผู้ดูแลระบบให้เร่งดำเนินการแพตช์ VMware ESXi เพื่อปิดช่องโหว่	วันที่ 9 กุมภาพันธ์ 2566

Singapore Computer Emergency Response Team (SingCert) มีการเผยแพร่รายงานเกี่ยวกับแคมเปญแรนซัมแวร์ ที่กำลังดำเนินอยู่ โดยการใช้ประโยชน์จากช่องโหว่เก่าหมายเลข (CVE-2021-21974) ในเซิร์ฟเวอร์ VMware ESXi ที่ไม่ได้รับการแพตช์

ผู้ใช้งานและผู้ดูแลระบบของเวอร์ชันที่ได้รับผลกระทบ จึงควรอัปเดตให้เป็นเวอร์ชันล่าสุด เพื่อเป็นการป้องกันจากการถูกโจมตี และขอให้ทำการตรวจสอบระบบทั้งหมด เพื่อสแกนหาสัญญาณของการบุกรุก ผู้ใช้งานและผู้ดูแลระบบควรประเมินด้วยว่าพอร์ต 427 บนระบบ ESXi สามารถปิดใช้งานได้ โดยไม่รบกวนการทำงานหรือไม่ อาจต้องกำหนดค่ากฎ Firewall โดยอ้างว่าถูกโจมตี เพื่อหยุดการเชื่อมต่อกับ ที่อยู่ IP ดังต่อไปนี้

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

ข้อมูลอ้างอิงช่องโหว่ : CVE-2021-21974

ระบบที่ได้รับผลกระทบ :

- 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

ระดับความรุนแรง (Severity) : High

ผลกระทบของช่องโหว่ : ผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่เพื่อทำการโจมตี โดยการเรียกใช้โค้ดจากระยะไกล ซึ่งเรียกว่า heap-overflow ในบริการ OpenSLP

วิธีการป้องกัน : ดำเนินการ Update Patch เป็นเวอร์ชันล่าสุด

ที่มาของข้อมูล :

https://www.csa.gov.sg/en/singcert/Alerts/AL-2023-015
https://www.opencve.io/cve/CVE-2021-21974
https://www.vmware.com/security/advisories/VMSA-2021-0002.html
https://www.bleepingcomputer.com/news/security/massive-esxiargs-ransomware-attack-targets-vmware-esxi-servers-worldwide/
https://www.cert.ssi.gouv.fr/alerte/CERTFR-2023-ALE-015/
https://www.csa.gov.sg/singcert/Advisories/ad-2021-009/

TLP : CLEAR