เอกสารการแจ้งเตือนกรณี VMware พบกลุ่มแรนซัมแวร์มุ่งเป้าโจมตี ESXi Server ที่ไม่ได้รับการแพตช์

การแจ้งเตือนกรณี VMware พบกลุ่มแรนซัมแวร์มุ่งเป้าโจมตี ESXi Server ที่ไม่ได้รับการแพตช์

VMware ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ออกแจ้งเตือนผู้ใช้งาน VMware ESXi Hypervisor ว่ากำลังพบการระบาดของแรนซัมแวร์ใน ESXi Server ที่ยังไม่ได้รับการแพตช์ โดยกลุ่มผู้ไม่หวังดีจะโจมตีผ่านช่องโหว่ CVE-2021-21974[1] ทำให้เกิด Heap overflow ใน OpenSLP ที่ใช้งานใน ESXi โดยการโจมตีนั้นเกิดขึ้นผ่านพอร์ต 427 โดยปกติแล้วจะถูกปิดเอาไว้ หากโจมตีสำเร็จจะมีการติดตั้งแรนซัมแวร์ลงในเครื่องของผู้ใช้งานและใช้เป็นช่องทางในการโจมตีต่อไป ซึ่ง ESXi ที่ได้รับผลระทบจากช่องโหว่ดังกล่าว ได้แก่

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

ทั้งนี้ ผู้ใช้งานหรือผู้ดูแลควรตรวจสอบและปฏิบัติตามคำแนะนำข้างต้นที่ https://www.cisa.gov/sites/default/files/2023-03/aa23-075a-stop-ransomware-lockbit.pdf เพื่อลดความเสี่ยงจากการโจมตี สามารถติดตามข้อมูลเพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://blog.checkpoint.com/2023/02/06/massive-ransomware-attack-targets-vmware-esxi-servers/
2. https://www.forescout.com/blog/vmware-esxi-servers-a-major-attack-vector-for-ransomware/

คำแนะนำสำหรับการตรวจสอบเพื่อลดความเสี่ยงจากการถูกโจมตี

ลำดับ	คำแนะนำ	มี	ไม่มี
1	เก็บข้อมูลสำรองที่สำคัญอย่างสม่ำเสมอ โดยการแยกจากระบบเครือข่ายหลัก		
2	อัปเดตแพตช์และซอฟต์แวร์ รวมถึงระบบปฏิบัติการและโปรแกรมป้องกันไวรัส ตรวจสอบให้แน่ใจว่ามีการติดตั้งแพตช์ล่าสุดสำหรับ VMware ESXi และซอฟต์แวร์ที่เกี่ยวข้องทั้งหมด		
3	ติดตั้งโปรแกรมป้องกันไวรัส รวมถึงตรวจสอบการเข้าถึงของระบบเพื่อตรวจพบกิจกรรมที่ผิดปกติ และดำเนินการตอบสนอง		
4	ใช้ไฟวอลล์เพื่อกรองการส่งข้อมูลเข้าและออก แบ่งเครือข่ายเพื่อจำกัดการแพร่กระจายของมัลแวร์		
5	การเข้าสู่ระบบต้องมีการตรวจสอบหลายขั้นตอน (MFA) สำหรับการเข้าสู่ระบบเพื่อป้องกันการโจมตีด้วย Phishing สำหรับทุกการใช้งาน โดยเฉพาะเว็บเมล เครือข่าย และบัญชีการเข้าใช้งานที่สำคัญ		
6	ปิดการใช้งานสคริปต์มาโครจากไฟล์ทำงานที่ถูกส่งผ่านทางอีเมล		
7	ใช้ VPN สำหรับการเข้าถึงระบบทางไกลที่ปลอดภัย และตรวจสอบการกำหนดค่าโปรโตคอลเดสก์ท็อประยะไกล (RDP) อย่างสม่ำเสมอ		
8	ใช้เครื่องมือ EDR เพื่อตรวจหาและตอบสนองต่อความเสี่ยงอย่างสม่ำเสมอ		

คำแนะนำสำหรับการฝึกอบรมและตระหนักของบุคลากรของหน่วยงาน

ลำดับ	คำแนะนำ	มี	ไม่มี
1	จัดการฝึกอบรมเป็นประจำเกี่ยวกับการรับรู้ Phishing		
2	ให้ความรู้แก่พนักงานเกี่ยวกับการใช้งานเว็บไซต์อย่างปลอดภัย การใช้รหัสผ่านที่ปลอดภัย และความสำคัญของการไม่ดาวน์โหลดหรือติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาต		
3	ฝึกอบรมพนักงานให้รายงานกิจกรรมที่น่าสงสัยหรือการละเมิดที่อาจเกิดขึ้นทันที		

แนวทางปฏิบัติของบุคลากรของหน่วยงาน เพื่อลดความเสี่ยงจากการถูกโจมตี

ลำดับ	คำแนะนำ	มี	ไม่มี
1	พัฒนาและปรับปรุงแผนการตอบสนองต่อเหตุการณ์อย่างสม่ำเสมอ และดำเนินการฝึกซ้อมจำลองสถานการณ์เพื่อให้แน่ใจว่ามีความพร้อม		
2	ดำเนินการตรวจสอบความปลอดภัยเป็นระยะเพื่อระบุและลดความเสี่ยงจากช่องโหว่		
3	ตรวจสอบให้แน่ใจว่าผู้จำหน่ายปฏิบัติตามหลักปฏิบัติด้านความปลอดภัยทางไซเบอร์ที่เข้มงวด		
4	พิจารณาประกันภัยทางไซเบอร์เพื่อลดผลกระทบทางการเงินจากการโจมตีแรนซัมแวร์		
5	ปฏิบัติตามกฎระเบียบและมาตรฐานความปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง		
6	ตรวจสอบเครือข่ายและระบบอย่างสม่ำเสมอเพื่อหากิจกรรมที่ผิดปกติ		

ลำดับ	คำแนะนำ	มี	ไม่มี
7	แบ่งปันข้อมูลด้านความปลอดภัยทางไซเบอร์ที่เกี่ยวข้องเพื่อรับข้อมูลภัยคุกคามล่าสุด		