ด่วนที่สุด

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศการประชาสัมพันธ์ กพช. โทร. ๐ ๒๖๑๘ ๒๓๒๓ ต่อ ๑๐๑๒

ที่ นร ๐๒๐๖.๐๓/ว๓๐๔ **วันที่** ๒๒ เมษายน ๒๕๖๕

เรื่อง แจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต

เรียน ผอ.สำนัก/กอง , ผอ.สปข. ๑-๘ , ปชส. ๗๖ จังหวัด และหัวหน้าหน่วยงานสังกัด กปส.

ตามหนังสือ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ที่ สกมช. ๐๘๒๐/๒๔๕ ลงวันที่ ๑๑ เมษายน ๒๕๖๕ เรื่อง การแจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต นั้น

ในการนี้ ศสช. ขอให้หน่วยงานในสังกัด กปส.ตรวจสอบว่าระบบ ซอฟต์แวร์หรืออุปกรณ์ที่ใช้มีการใช้งาน VMware ดังต่อไปนี้หรือไม่

๑. VMware Tanzu Application Service for VMs (TAS)

๒. VMware Tanzu Operation Manager (Ops Manager)

๓. VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

หากมีการใช้งานควรอัปเดตให้เป็นเวอร์ชันล่าสุด เพื่อความปลอดภัยและลดผลกระทบในการถูกโจมตี

จึงเรียนมาเพื่อโปรดทราบ และดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นางสาวอรัญญา เกตุแก้ว)

ผอ.ศสช.

TLP: WHITE

ส่ง สสช.
19 เม.ย. 65

กระดาษเขียนข่าว

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ความเร่งด่วน-ผู้รับปฏิบัติ		ลำดับความเร่งด่วน-ผู้รับทราบ	วัน เวลา	คำแนะนำในการส่งข่าว
ด่วนที่สุด		ด่วนที่สุด	๑๑ เมษายน ๒๕๖๕	
จาก	ผู้อำนวยการศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ			
ถึง	ผู้รับปฏิบัติ	ผู้ดูแลระบบ หรือผู้ที่เกี่ยวข้อง		ชั้นความลับ
	ผู้รับทราบ	หัวหน้าส่วนราชการ		ที่ของผู้ให้ข่าว ที่ สกมช ๐๘๒๐/๒๙๕

๑. เพื่อกรุณาทราบ

๒. ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์และได้ตรวจพบว่า มีการประกาศเผยแพร่ช่องโหว่ระดับวิกฤติ "Spring4Shell" และ "Spring Cloud Function" ซึ่งสามารถโจมตีแบบรันคำสั่งจากระยะไกล Remote code execution (RCE) เพื่อควบคุมเครื่องที่ตกเป็นเหยื่อได้ จึงขอให้ท่านตรวจสอบและดำเนินการป้องกันความเสียหายที่อาจเกิดขึ้นได้ ทั้งนี้ หากมีข้อสงสัยสามารถติดต่อสอบถามเพิ่มเติมได้ที่ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) หมายเลขโทรศัพท์ ๐๘ ๐๓๓๙ ๙๓๗๘ หรือ E-mail : ncert@ncsa.or.th

หมายเหตุ รายละเอียดเพิ่มเติมปรากฏตามเอกสารแจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต

หน้า ๑ ของ ๑ หน้า	อ้างถึงข่าว	ผู้เขียนข่าว	หน่วย	โทรศัพท์
	ชั้นความลับ [ ] กำหนด [/] ไม่กำหนด	พ.ต.อ. (ณัทกฤช พรหมจันทร์)	ศปช.	๐๘ ๐๓๓๙ ๙๓๗๘
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ		ผู้อนุมัติข่าว น.อ. (อมร ชมเชย) รอง ลธ.กมช.(๔)/ผอ.ศปช.		

เอกสารการแจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต

ตามกระดาษเขียนข่าวที่ สกมช 0820/245 ลงวันที่ 11 เมษายน 2565

การแจ้งเตือนช่องโหว่ "Spring4Shell" ผู้ดูแลระบบควรตรวจสอบและอัปเดตทันที

เมื่อวันที่ 1 เมษายน 2565 Cybersecurity and Infrastructure Security Agency (CISA) พบช่องโหว่ระดับวิกฤตที่ส่งผลกระทบต่อระบบปฏิบัติการที่มีการใช้งาน Spring Framework และ Spring Cloud Function[1] จำนวน 2 ช่องโหว่ คือช่องโหว่หมายเลข CVE-2022-22963[2] และช่องโหว่หมายเลข CVE-2022-22965[3] โดยช่องโหว่ดังกล่าวทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องของผู้ถูกโจมตีโดยวิธีการ Remote code execution (RCE) และสามารถทำการขโมยข้อมูลภายในเครื่องของผู้ที่ถูกโจมตีได้

ช่องโหว่ Spring4Shell (CVE-2022-22965) เป็นช่องโหว่บน Spring Framework ของ Java มีความร้ายแรงของภัยคุกคามในระดับวิกฤต[4] ช่องโหว่ดังกล่าวทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงเครื่องของผู้ถูกโจมตีโดยวิธี RCE และขโมยข้อมูลภายในเครื่องของผู้ที่ถูกโจมตีได้ จึงขอความร่วมมือให้หน่วยงานภาครัฐและภาคเอกชน ตรวจสอบว่าระบบ ซอฟต์แวร์ หรืออุปกรณ์ที่ใช้อยู่ มีการใช้งาน VMware ดังต่อไปนี้หรือไม่

1. VMware Tanzu Application Service for VMs (TAS)
2. VMware Tanzu Operations Manager (Ops Manager)
3. VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

หากมีการใช้งานควรอัปเดตให้เป็นเวอร์ชันล่าสุด เพื่อความปลอดภัยและลดผลกระทบในการถูกโจมตีได้ ในปัจจุบันได้มีการรายงานบนสื่อสังคมออนไลน์ต่าง ๆ ว่าได้เริ่มมีการโจมตีโดยใช้ช่องโหว่ดังกล่าวนอกจากจะโจมตีแบบรันคำสั่งจากระยะไกล (RCE) เพื่อควบคุมเครื่องแล้ว ยังมีการปล่อยมัลแวร์เพื่อใช้เครื่องที่ถูกยึดได้ โจมตีระบบงานหรือเครื่องแม่ข่ายอื่น ๆ ต่อไปอีกด้วย ผู้ดูแลระบบควรเฝ้าระวังการโจมตีโดยอาศัยช่องโหว่ดังกล่าวในระบบภายในหน่วยงานและควร Patch ระบบปฏิบัติการ แอปพลิเคชัน อุปกรณ์รักษาความปลอดภัยต่าง ๆ ให้ทันสมัยอยู่เสมอเพื่อลดผลกระทบที่อาจจะเกิดขึ้นด้วย

อ้างอิง

1. https://www.cisa.gov/uscert/ncas/current-activity/2022/04/01/spring-releases-security-updates-addressing-spring4shell-and
2. https://tanzu.vmware.com/security/cve-2022-22963
3. https://tanzu.vmware.com/security/cve-2022-22965
4. https://www.vmware.com/security/advisories/VMSA-2022-0010.html