หนังสือฉบับนี้พิมพ์จาก
ระบบสารบรรณ/หนังสือเวียนกรุงเทพมหานคร
วันที่ ๑๐ พ.ค. ๒๕๖๕

สำนักงานเขตลาดกระบัง
เลขรับ ๗๖๖
วันที่ ๑๐ พ.ค. ๒๕๖๕
เวลา ๑๓.๒๖

สำนักงานเขตลาดกระบัง
รับที่ ๓๖๒๓
วันที่ ๒๕ พ.ค. ๒๕๖๕
เวลา ๐๙.๖๗

บันทึกข้อความ

ส่วนราชการ สำนักยุทธศาสตร์และประเมินผล (กองควบคุมระบบคอมพิวเตอร์ โทร. ๐๔ ๑๖๑๙ ๙๒๐๙)

ที่ กท ๐๕๐๘/ ๘๗๒ **วันที่** ๓ พฤษภาคม ๒๕๖๕

เรื่อง การแจ้งช่องโหว่ Spring4Shell และ Spring Cloud Function บน Spring Framework ของ Java

เรียน ผู้อำนวยการสำนัก หัวหน้าสำนักงาน ก.ก. หัวหน้าผู้ตรวจราชการกรุงเทพมหานคร ผู้ช่วยปลัดกรุงเทพมหานคร เลขานุการสภากรุงเทพมหานคร เลขานุการผู้ว่าราชการกรุงเทพมหานคร ผู้อำนวยการเขต หัวหน้าส่วนราชการในสังกัดสำนักปลัดกรุงเทพมหานคร และผู้อำนวยการสำนักงานการพาณิชย์ของกรุงเทพมหานคร

ด้วยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) ได้ประกาศเตือนเกี่ยวกับการโจมตีผ่านช่องโหว่ Spring4Shell และ Spring Cloud Function ซึ่งเป็นช่องโหว่บน Spring Framework ของ Java ที่มีความร้ายแรงของภัยคุกคามในระดับวิกฤติ ช่องโหว่ดังกล่าวอาจส่งผลให้ผู้ประสงค์ร้ายสามารถเข้าถึงเครื่องของผู้ถูกโจมตีโดยวิธี RCE (Remote Code Execution) ได้

สำนักยุทธศาสตร์และประเมินผลได้รับการแจ้งเตือนดังกล่าว จึงขอให้หน่วยงานของกรุงเทพมหานคร ตรวจสอบว่าระบบซอฟต์แวร์ หรืออุปกรณ์ของท่านมีการใช้งาน VMware ดังต่อไปนี้หรือไม่

๑. VMware Tanzu Application Service for VMs (TAS)
๒. VMware Tanzu Operations Manager (Ops Manager)
๓. VMware Tanzu Kubernetes Grid Integrated Edition (TKGI)

หากมีการใช้งานขอให้หน่วยงานทำการอัพเดตซอฟต์แวร์ดังกล่าวให้เป็นเวอร์ชันล่าสุด ตามคำแนะนำศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) แนะนำ รายละเอียดตามเอกสารที่แนบ

จึงเรียนมาเพื่อโปรดดำเนินการในส่วนที่เกี่ยวข้องต่อไป

(นายแสนยากร อุ่นมีศรี)
ผู้อำนวยการสำนักยุทธศาสตร์และประเมินผล

เรียน ผู้อำนวยการเขตลาดกระบัง
- เพื่อโปรดพิจารณา
- เห็นควรให้ ฝ่ายปกครอง
ดำเนินการต่อไป

(นายสกนธ์ ตระกูลวงศ์บุญมา)
นักประชาสัมพันธ์ชำนาญการ รักษาการในตำแหน่ง
หัวหน้าฝ่ายปกครอง สำนักงานเขตลาดกระบัง
๑๘ พ.ค. ๒๕๖๕

๔.ปกครอง
แจ้งเวียน

ผู้ช่วยผู้อำนวยการเขต ปฏิบัติราชการแทน
ผู้อำนวยการเขตลาดกระบัง
๑๘ พ.ค. ๒๕๖๕

(นางโชติกา กิตติรัตนกรกุล)
นักจัดการงานทั่วไป...
หัวหน้าฝ่ายปกครอง...
๑๐ พ.ค. ๒๕๖๕

ที่ กท ๕๓๐๑/๑๐๙๔ ลงวันที่ ๒๔ พ.ค. ๒๕๖๕
เรียน หัวหน้าฝ่าย ทุกฝ่าย

☑ สำเนาถูกต้องเพื่อโปรดทราบ
☑ และดำเนินการในส่วนที่เกี่ยวข้อง
☐ หากเป็นประการใด แจ้งฝ่ายปกครอง ทราบภายในวันที่.....
☐ ดูรายละเอียดที่ฝ่ายปกครอง

(นายทศพล ศิวลัย)
นักทรัพยากรบุคคลชำนาญการ รักษาการในตำแหน่ง
หัวหน้าฝ่ายปกครอง สำนักงานเขตลาดกระบัง

คุณยุพิน

(นายปราโมทย์ สีธูป)
นักวิชาการศึกษาชำนาญการพิเศษ
หัวหน้าฝ่ายการศึกษา สำนักงานเขตลาดกระบัง

ที่ กท ๕๓๐๗/ [illegible] ลงวันที่ ๒๗ พ.ค. ๒๕๖๕
เรียน ผู้อำนวยการสถานศึกษาที่เกี่ยวข้องทุกแห่ง

☑ [illegible]
☐ [illegible]
☐ ส่งข้อมูลให้ฝ่ายการศึกษาทราบ
☐ ภายในวันที่.....

(นายปราโมทย์ สีธูป)
นักวิชาการศึกษาชำนาญการพิเศษ
หัวหน้าฝ่ายการศึกษา สำนักงานเขตลาดกระบัง

สำนักยุทธศาสตร์
รับที่ 1788
วันที่ 20 เม.ย. 2565
เวลา 10.20

เลขรับ 1446
วันที่ 20 เม.ย. 2565
เวลา 10.53

รับที่ ๑๙ เม.ย. ๒๕๖๕
เวลา ๑๖.๑๕

TLP: WHITE

กรุงเทพมหานคร
เลขที่ 12897
วันที่ 19 เม.ย. 2565
เวลา 15.54 น.

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

<u>หมายเหตุ</u> รายละเอียดเพิ่มเติมปรากฏตามเอกสารแจ้งเตือนกรณีมีการเผยแพร่ช่องโหว่ระดับวิกฤต

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

TLP: WHITE

กองควบคุมระบบคอมพิวเตอร์
สยป.ทหม. 918
รับที่ ๒๑ เมย ๒๕๖๕
เวลา

เรียน ผอ.สยป.
พิจารณาดำเนินการ ในส่วนที่เกี่ยวข้อง

(นายขจิต ชัชวานิชย์)
ปลัดกรุงเทพมหานคร
๑๙ เม.ย. ๒๕๖๕

เรียน ผู้อำนวยการสำนักยุทธศาสตร์และประเมินผล
เพื่อโปรดทราบ และเห็นควร
ชอบ กคม พิจารณาดำเนินการ

(นายชลวิทย์ เชื้อหอม)
เลขานุการสำนัก
สำนักยุทธศาสตร์และประเมินผล
20 เม.ย. 2565

ชอบ กคม.
(นายแสนยากร อุ่นมีศรี)
ผู้อำนวยการสำนักยุทธศาสตร์และประเมินผล
๒๐ เม.ย. ๒๕๖๕

☑ ห.ฝ่ายระบบเครื่องและเครือข่าย ☑ พิจารณา ☐ .....
☐ ห.ฝ่ายโปรแกรมระบบ ☐ ดำเนินการ ☐ .....
☑ ห.ฝ่ายฐานข้อมูล ☐ ทราบ ☐ .....
☐ หงานธุรการ ☐ เวียน ☐ .....

(นายมนตรี ส่งวุฒิวงศากร)
ผู้อำนวยการกองควบคุมระบบคอมพิวเตอร์
สำนักยุทธศาสตร์และประเมินผล

เรียน คุณหศ.ปรัย
- ตั้งค่ากำแพงกันที่ Firewall
- แจ้งเวียนทุกหน่วยงาน

(นายเปรมชาย จงเจริญ)
หัวหน้าฝ่ายฐานข้อมูล
กองควบคุมระบบคอมพิวเตอร์
สำนักยุทธศาสตร์และประเมินผล

TLP: WHITE

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 ว่าได้เริ่มมีการโจมตีโดยใช้ช่องโหว่ดังกล่าว นอกจากจะโจมตีแบบรับคำสั่งจากระยะไกล (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

TLP: WHITE