แจ้งเตือน : ช่องโหว่

Spring Core Framework Zero Day

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☐ Non-compliance
- ☐ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ประเภท Zero-Day ใน Module Core ของ Java Spring Framework สำหรับพัฒนา Java Web Application (Spring4Shell)

วันที่แจ้งเตือน 31 มีนาคม 2565

ตามที่ปรากฏเป็นข่าวแจ้งเตือนข่าวเกี่ยวกับช่องโหว่ประเภท Zero-Day ใน Module Core ของ Java Spring Framework สำหรับพัฒนา Java Web Application (Spring4Shell) ผู้ไม่หวังดีสามารถใช้เทคนิคการปลอมแปลงการเรียกใช้งาน Http Request ส่งผลให้สามารถเรียกใช้คำสั่งระยะไกลโดยไม่ได้รับอนุญาต (Remote Code Execution)

นักวิจัยด้านการรักษาความปลอดภัยได้ทำการ Proof of Concept (POC) แล้วพบว่าช่องโหว่ดังกล่าวไม่ซับซ้อนและสามารถใช้งานได้จริงบน Spring Framework โดยเวอร์ชันที่ได้รับผลกระทบตั้งแต่เวอร์ชัน 9 เป็นต้นมา

ในปัจจุบันเจ้าของผลิตภัณฑ์ยังไม่ได้มีการออก Security Patch เพื่อแก้ไขช่องโหว่ดังกล่าว เพื่อหลีกเลี่ยงและป้องกันความเสี่ยงที่อาจเกิดขึ้น ผู้ดูแลระบบควรพิจารณาดำเนินการดังนี้

1) ผู้ดูแลระบบสามารถใช้วิธีการเพื่อที่จะลดความเสี่ยงเบื้องต้น (Workaround) โดยทำการตั้งค่าการตรวจจับและกรองการเรียกใช้ "class.*" "Class.*" "*.class.*" และ "*.Class.*“ ใน Spring Framework Databinder หรืออุปกรณ์ Web Application Firewall (WAF) โดยสามารถศึกษารายละเอียดได้ใน URL ที่อ้างอิง
2) ติดตามการออก Security Patch อย่างใกล้ชิดเพื่อให้สามารถลดความเสี่ยงที่ใช้ช่องโหว่ดังกล่าวโจมตีองค์กรได้อย่างทันการณ์
3) ผู้ดูแลระบบควรประเมินความเสี่ยงจากการใช้วิธีแก้ไขความเสี่ยงชั่วคราว (Workaround) รวมถึงการตั้งค่าการป้องกันบนอุปกรณ์รักษาความปลอดภัย เพื่อประเมินผลกระทบต่อการทำงานของระบบงานที่ใช้ Java Web Application ดังกล่าวก่อนนำไปติดตั้งบนระบบที่ให้บริการจริง

แจ้งเตือน : ช่องโหว่

Spring Core Framework Zero Day

ผลกระทบทางธุรกิจ

- ☒ Financial Damage
- ☒ Reputation Damage
- ☐ Non-compliance
- ☐ Privacy Violation

ผลกระทบต่อระบบ

- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : White

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ประเภท Zero-Day ใน Module Core ของ Java Spring Framework สำหรับพัฒนา Java Web Application (Spring4Shell)

วันที่แจ้งเตือน 31 มีนาคม 2565

ข้อมูลอ้างอิง *External Link*

1) Workaround
   1.1. https://github.com/lunasec-io/lunasec/blob/master/docs/blog/2022-03-30-spring-core-rce.mdx?fbclid=IwAR0Vo4rIyfiPZhH50_sUzfAXIjibKxkmspT1Y2s03GvWX1-1Z_2yO_O-ir8
   1.2. https://www.praetorian.com/blog/spring-core-jdk9-rce/
2) https://www.cyberkendra.com/2022/03/springshell-rce-0-day-vulnerability.html (Firewall Rule)
3) https://www.cyberkendra.com/2022/03/spring4shell-details-and-exploit-code.html
4) https://www.scmagazine.com/news/cloud-security/critical-rce-vulnerability-spring4shell-found-in-spring-cloud-function%EF%BF%BC
5) https://threatpost.com/critical-rce-bug-spring-log4shell/179173/