แจ้งเตือน

Alert

ผลกระทบทางธุรกิจ

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

ผลกระทบต่อระบบ

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

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

Amazon Web Services (AWS) ออก Security Patch แก้ไขช่องโหว่ใน Research and Engineering Studio (RES) หลายรายการ

วันที่แจ้งเตือน 11 เมษายน 2569

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน ก.ล.ต.) และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ภาคตลาดทุน (TCM-CERT) ได้ติดตามข่าวสารและพบว่า Amazon Web Services (AWS) ออก Security Patch แก้ไขช่องโหว่ร้ายแรง 3 รายการ ในระบบ Research and Engineering Studio (RES) ซึ่งผู้ไม่หวังดีสามารถใช้โจมตีแบบ Remote Code Execution ด้วยสิทธิ์ระดับ root ได้ ได้แก่

1. CVE-2026-5707 เป็นช่องโหว่ประเภท OS command injection เกิดจากการตรวจสอบข้อมูลนำเข้า session ของ Virtual Desktop ที่ไม่เหมาะสม ทำให้ผู้ไม่หวังดีสามารถรันคำสั่งด้วยสิทธิ์ Root บนโฮสต์ได้
2. CVE-2026-5708 เป็นช่องโหว่การควบคุมสิทธิ์ที่ไม่เหมาะสมในกระบวนการสร้าง session ทำให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ์และเข้าถึงทรัพยากร AWS อื่นได้โดยไม่ได้รับอนุญาต
3. CVE-2026-5709 เป็นช่องโหว่ OS command injection ใน FileBrowser API ซึ่งอาจถูกใช้รันคำสั่งบนระบบ cluster-manager EC2

การโจมตีจะต้องอาศัยบัญชีผู้ใช้งานที่ผ่านการยืนยันตัวตนก่อน อย่างไรก็ดี ช่องโหว่ดังกล่าวสามารถถูกใช้เป็นช่องทางในการยึดครองระบบ virtual desktop เข้าควบคุม cluster manager และขยายการโจมตีไปยังทรัพยากรสำคัญอื่นในระบบคลาวด์ ซึ่งอาจส่งผลให้เกิดความเสี่ยงด้านการรั่วไหลของข้อมูล การถูกควบคุมระบบ และการหยุดชะงักของการดำเนินงานของหน่วยงานได้

เพื่อป้องกันและลดความเสี่ยงจากช่องโหว่ดังกล่าว สำนักงาน ก.ล.ต. และ TCM-CERT ขอให้ผู้ประกอบธุรกิจและผู้ดูแลระบบที่ใช้ผลิตภัณฑ์ดังกล่าว พิจารณาดำเนินการตรวจสอบและอัปเกรด RES เป็นเวอร์ชัน 2026.03 หรือเวอร์ชันที่ผู้ผลิตแนะนำ ทั้งนี้ หากยังไม่สามารถอัปเกรดได้ ขอให้พิจารณาดำเนินการตามแนวทางแก้ไขชั่วคราวตามที่ AWS เผยแพร่ เพื่อป้องกันช่องโหว่ command injection และ privilege escalation และตรวจสอบและอัปเดตนโยบายการตั้งค่าความปลอดภัยของระบบ ปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยให้สอดคล้องกับภัยคุกคามล่าสุด

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อหน่วยงานในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1. https://cybersecuritynews.com/aws-patches/
2. https://nvd.nist.gov/vuln/detail/CVE-2026-5707
3. https://nvd.nist.gov/vuln/detail/CVE-2026-5708
4. https://nvd.nist.gov/vuln/detail/CVE-2026-5709
5. https://aws.amazon.com/security/security-bulletins/2026-014-aws/