วันที่ 16 กันยายน 2568

ช่องโหว่ร้ายแรง CVE-2025-5086 ใน DELMIA Apriso ถูกใช้โจมตีจริงแล้ว CISA ออกประกาศเตือน

CISA (Cybersecurity and Infrastructure Security Agency) หรือหน่วยงานความมั่นคงปลอดภัยไซเบอร์ของสหรัฐฯ ได้เพิ่มช่องโหว่ร้ายแรงที่กระทบต่อซอฟต์แวร์ Dassault Systèmes DELMIA Apriso Manufacturing Operations Management (MOM) ลงในบัญชี Known Exploited Vulnerabilities (KEV) หลังจากพบหลักฐานว่ามีการโจมตีเกิดขึ้นจริงในโลกออนไลน์

ช่องโหว่นี้ถูกติดตามในชื่อ CVE-2025-5086 โดยมีคะแนนความรุนแรง CVSS 9.0 จาก 10.0 จัดอยู่ในระดับวิกฤต ตามข้อมูลจาก Dassault ระบุว่าช่องโหว่นี้ส่งผลกระทบกับซอฟต์แวร์ตั้งแต่เวอร์ชัน Release 2020 จนถึง Release 2025

กลไกการโจมตีที่ซับซ้อน

“Dassault Systèmes DELMIA Apriso มีช่องโหว่การจัดการข้อมูลที่ไม่ได้รับการตรวจสอบก่อนนำไปใช้ (deserialization of untrusted data) ซึ่งอาจนำไปสู่การสั่งรันโค้ดจากระยะไกลได้” CISA กล่าวไว้ในประกาศ การเพิ่ม CVE-2025-5086 เข้าสู่บัญชี KEV เกิดขึ้นหลังจากที่ SANS Internet Storm Center รายงานการพยายามโจมตีที่มุ่งเป้าช่องโหว่นี้โดยมาจากไอพี 156.244.33[.]162 ซึ่งระบุตำแหน่งว่าอยู่ที่เม็กซิโก

การโจมตีทำโดยการส่งคำขอ HTTP ไปยังจุดเชื่อมต่อ "/apriso/WebServices/FlexNetOperationsService.svc/Invoke" พร้อมเพย์โหลดที่เข้ารหัสแบบ Base64 ซึ่งเมื่อถอดรหัสจะได้ไฟล์ที่บีบอัดด้วย GZIP และข้างในเป็นไฟล์ DLL ของ Windows ชื่อ "fwitxz01.dll"

Trojan ที่ทำหน้าที่สอดแนม

Kaspersky ตรวจพบว่า DLL ดังกล่าวคือมัลแวร์ "Trojan.MSIL.Zapchast.gen" ซึ่งถูกออกแบบมาเพื่อสอดแนมกิจกรรมของผู้ใช้ ไม่ว่าจะเป็นการดักจับการพิมพ์คีย์บอร์ด, การแคปหน้าจอ และการเก็บรายชื่อโปรแกรมที่กำลังใช้งานอยู่

“ข้อมูลที่เก็บได้จะถูกส่งกลับไปยังผู้ไม่หวังดีผ่านหลายช่องทาง ทั้งอีเมล, FTP และ HTTP (โดยส่งข้อมูลไปในคำขอ)” บริษัทด้านความปลอดภัยไซเบอร์จากรัสเซียกล่าวเพิ่มเติม

สำหรับตระกูลมัลแวร์ Zapchast ตามรายงานของ Bitdefender และ Trend Micro เคยถูกแพร่กระจายผ่านอีเมลฟิชชิ่งที่แนบไฟล์อันตรายมาตั้งแต่กว่าทศวรรษที่ผ่านมา และยังไม่ชัดเจนว่า "Trojan.MSIL.Zapchast.gen" เป็นเวอร์ชันที่พัฒนาต่อมาหรือไม่ ด้วยเหตุการณ์ที่มีการโจมตีจริงในหน่วยงาน Federal Civilian Executive Branch (FCEB) ได้รับคำแนะนำให้ติดตั้งอัปเดตที่จำเป็นภายในวันที่ 2 ตุลาคม 2025 เพื่อป้องกันเครือข่ายของตนเอง

ข้อมูลอ้างอิง

Sep 12, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/09/critical-cve-2025-5086-in-delmia-apriso.html