วันที่ 4 มีนาคม 2568

ช่องโหว่ RCE ที่อยู่ในระดับ Critical ใน Apache Parquet

Executive Summary

ช่องโหว่ร้ายแรงประเภท Remote Code Execution (RCE) ได้ถูกค้นพบใน Apache Parquet ทุกเวอร์ชั่นจนถึงเวอร์ชั่น 1.15.0 ซึ่งปัญหานี้เกิดจากการแปลงข้อมูลที่ไม่น่าเชื่อถือ (deserialization) ทำให้ผู้ไม่หวังดีสามารถรันโค้ดอันตรายบนระบบเป้าหมายได้ ช่องโหว่นี้อาจนำไปสู่การยึดระบบ ขโมยหรือแก้ไขข้อมูล หรือปล่อยมัลแวร์ ซึ่งช่องโหว่นี้ถูกติดตามภายใต้รหัส CVE-2025-30065 และได้รับการแก้ไขแล้วใน Apache Parquet เวอร์ชั่น 1.15.1

Vulnerability detail (รายละเอียดช่องโหว่)

ช่องโหว่ด้านความปลอดภัยนี้เกี่ยวกับ Apache Parquet ที่ระบุเป็น CVE-2025-30065 จัดอยู่ในประเภท Deserialization of Untrusted Data (CWE-502) และมีระดับความรุนแรงสูงสุด (CVSS 10.0, “ร้ายแรง”) ช่องโหว่นี้สามารถส่งผลกระทบต่อข้อมูลในระบบและการวิเคราะห์ที่นำเข้าไฟล์ Parquet โดยเฉพาะเมื่อไฟล์เหล่านี้มาจากแหล่งภายนอกหรือแหล่งที่ไม่น่าเชื่อถือ ทำให้ผู้โจมตีสามารถแทรกไฟล์และทำให้ช่องโหว่ดังกล่าวอาจถูกเรียกใช้งานได้

เวอร์ชั่นผลิตภัณฑ์ที่ได้รับผลกระทบและแพตช์ (Affected version and patch)

- Apache Parquet เวอร์ชัน ตั้งแต่ 1.8.0 จนถึง 1.15.0
- ความเสี่ยงต่อการถูกโจมตีแบบ Remote Code Execution (RCE) ผ่านไฟล์ Parquet ที่ถูกสร้างขึ้น

คำแนะนำ (Recommendation)

- ดำเนินการอัปเกรดเป็น Apache Parquet 1.15.1 ซึ่งเป็นเวอร์ชั่นที่ได้รับการแก้ไขช่องโหว่ CVE-2025-30065 แล้ว
- หลีกเลี่ยงการนำเข้าไฟล์ Parquet จากแหล่งที่ไม่เชื่อถือ
- ตรวจสอบความปลอดภัยของไฟล์ก่อนนำไปนำไปใช้งาน

ข้อมูลอ้างอิง

- https://www.bleepingcomputer.com/news/security/max-severity-rce-flaw-discovered-in-widely-used-apache-parquet/