

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

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



## แจ้งเตือนช่องโหว่ร้ายแรงบนซอฟต์แวร์บีบอัดข้อมูล XZ Utils (CVE-2024-3094)

วันที่แจ้งเตือน 10 เมษายน 2567

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงบนซอฟต์แวร์บีบอัดข้อมูล XZ Utils (CVE-2024-3094) ซึ่งเป็นชุดซอฟต์แวร์บีบอัดข้อมูลที่มีการใช้งานอย่างแพร่หลายบนระบบปฏิบัติการ Linux ส่งผลให้ผู้ไม่หวังดีสามารถเข้าสู่ระบบจากระยะไกลได้โดยไม่ได้รับอนุญาต (unauthorized access)

เวอร์ชันของ Library XZ Utils ที่ได้รับผลกระทบได้แก่

- XZ Utils เวอร์ชัน 5.6.0
- XZ Utils เวอร์ชัน 5.6.1

Red Hat ได้ออกประกาศเตือนให้หยุดการใช้งาน Fedora Linux 40 และ Fedora Rawhide ทันที และแนะนำให้ downgrade การใช้งาน XZ Utils เป็นเวอร์ชันที่ไม่มีช่องโหว่ เช่น 5.4.6 เป็นต้น เพื่อป้องกันการถูกโจมตีจากการใช้งานเวอร์ชันที่มีช่องโหว่

ทั้งนี้ กรณีผู้ประกอบการธุรกิจที่ใช้ชุดซอฟต์แวร์ดังกล่าว ควรพิจารณาอัปเดตเวอร์ชันของ Library XZ Utils ตามที่ Red Hat แนะนำ โดยควรประเมินความเสี่ยงและดำเนินการทดสอบก่อนนำไปใช้งานจริง พร้อมทั้งจัดให้มีมาตรการควบคุมอย่างเหมาะสมเพื่อป้องกันผลกระทบที่อาจเกิดขึ้น

### ข้อมูลอ้างอิง

- รายงานการแจ้งเตือนของคุณ์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 9 เม.ย. 2567
- <https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users>
- <https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094>
- <https://thehackernews.com/2024/03/urgent-secret-backdoor-found-in-xz.html>

ก.ล.ต. ดูแลตลาดทุน เพื่อให้คุณมั่นใจ