สรุปข่าวสาร IT Security ประจำสัปดาห์

วันที่ 25 - 31 ตุลาคม พ.ศ.2565

1. **WithSecure เตือน! กลไกเข้ารหัสของ Office 365 แฮกได้ง่ายมาก**

นักวิชาการจากบริษัทด้านความปลอดภัยทางไซเบอร์ WithSecure ได้ออกประกาศเตือนผู้ใช้ Office 365 ว่าระบบเข้ารหัสข้อความเมล Microsoft Office 365 Message Encryption (OME) สามารถโดนแฮกถอดรหัสได้ง่ายโดยไม่ต้องมีคีย์ ฟีเจอร์นี้อยู่ในชุด Office 365 ที่ให้ลูกค้าองค์กรส่งข้อความแบบเข้ารหัสในรูปของไฟล์แนบ HTML ในอีเมลได้ ซึ่งไมโครซอฟท์โฆษณาว่ามีประโยชน์มากในการส่งต่อข้อมูลที่เป็นความลับ อย่างเช่น ข้อมูลทางการแพทย์ แต่ทาง WithSecure ระบุว่าฟีเจอร์นี้ใช้กลไกเข้ารหัสที่ยังไม่ปลอดภัยเพียงพอ ทำให้ผู้ไม่หวังดีเข้ามาจัดการข้อความได้ ข้อความแบบ OME นี้ถูกสร้างขึ้นด้วย Electronic Codebook (ECB) ที่แบ่งส่วนข้อความออกเป็น Cipher Block ย่อยๆ แต่ละบล็อกจะถูกเข้ารหัสด้วยคีย์ที่จัดเก็บและจัดการโดยไมโครซอฟท์เอง ผ่านตัว Azure Rights Management (Azure RMS) แต่การที่จำนวนบล็อกของข้อความก่อนเข้ารหัสเหมือนกับหลังเข้ารหัสเป๊ะๆ จึงสามารถนำไปเดาต่อได้ง่าย

ข้อมูลจาก : < https://www.enterpriseitpro.net/office-365-encryption-easily-hacked-withsecure/ > 27/10/2022

2. **OpenSSL เตรียมออกอัปเดตอุดช่องโหว่ใหม่ระดับ Critical**

ทีมผู้พัฒนา OpenSSL ได้ประกาศผ่านทาง Mailing list ถึงแผนในการออกอัปเดตใหม่ เวอร์ชัน 3.0.7 เพื่ออุดช่องโหว่ระดับ Critical ซึ่งเป็นช่องโหว่ระดับความรุนแรงมากที่สุด ปัจจุบันยังไม่มีรายละเอียดเกี่ยวกับช่องโหว่มากนัก เนื่องจากตามนโยบายของ OpenSSL รายละเอียดของช่องโหว่จะถูกเก็บเป็นความลับ เพื่อเลี่ยงต่อการโจมตีที่อาจเกิดขึ้นในวงกว้าง โดยจะมีการแจ้งเตือนและส่งรายละเอียดช่องโหว่ไปที่ผู้ผลิตรายอื่นที่มีการใช้งาน OpenSSL ในระบบปฏิบัติการหรือซอฟต์แวร์ของตนเอง เพื่อให้ทำการแพตช์และแก้ไขปัญหาดังกล่าวล่วงหน้า ซึ่งตามนิยามของ OpenSSL แล้ว ช่องโหว่ระดับนี้ อาจถูกโจมตีได้ในการตั้งค่าแบบปกติ ทำให้ผู้ไม่หวังดีสามารถเจาะผ่านการ Remote และเข้าถึงข้อมูลที่สำคัญ

ข้อมูลจาก : < https://www.techtalkthai.com/openssl-will-releases-critical-vulnerability-patch/ > 27/10/2022

3. **Cisco เตือน พบการโจมตีผ่านช่องโหว่ใน AnyConnect Client บน Windows**

Cisco ได้ออกประกาศเตือนถึงช่องโหว่ใน Cisco AnyConnect Secure Mobility Client for Windows จำนวน 2 ตัว ได้แก่ CVE-2020-3433 และ CVE-2020-3153 มีความรุนแรงตาม CVSS score 7.8 และ 6.5 ตามลำดับ ถูกพบตั้งแต่สองปีที่แล้ว ทำให้ผู้ที่ทำการโจมตีจากภายในสามารถทำ DLL hijacking และวางไฟล์ไว้ใน System directory ได้ด้วยสิทธิระดับ System-level อย่างไรก็ตามช่องโหว่นี้ผู้โจมตีจำเป็นต้องมี Credential สำหรับเข้าสู่เครื่องก่อนจึงจะสามารถโจมตีได้ ทำให้ความรุนแรงไม่สูงมากนัก แต่เมื่อผู้โจมตีอาศัยช่องโหว่อื่นๆ เช่น Windows Privilege Escalation อาจทำให้เกิดความเสียหายมากได้ ล่าสุด Cisco PSIRT ได้รายงานว่าพบการโจมตีผ่านช่องโหว่นี้แล้ว นอกจากนี้ CISA ยังได้เพิ่มช่องโหว่นี้เข้าไปใน Know Exploited Vulnerability catalog เพื่อเฝ้าระวังอีกด้วย ผู้ใช้งานจึงควรทำการอัปเกรดเป็นเวอร์ชัน 4.9.00086 ขึ้นไปเพื่ออุดช่องโหว่ดังกล่าว

ข้อมูลจาก : < https://www.techtalkthai.com/cisco-warns-vulnerability-on-anyconnect-windows-client-being-exploited-in-the-wild/> 27/10/2022