สรุปข่าวสาร IT Security ประจำสัปดาห์

วันที่ 15 - 21 พฤศจิกายน พ.ศ.2565

1 ไมโครซอฟท์อุดช่องโหว่ Zero-day บนเอ็กซ์เชนจ์ “ProxyNotShell” แล้ว

ไมโครซอฟท์ปล่อยตัวอัปเดตด้านความปลอดภัยมาแก้ปัญหาช่องโหว่ Zero-day ร้ายแรงสองรายการบน Microsoft Exchange ที่รู้จักกันในชื่อ ProxyNotShell ที่ระบาดในวงกว้างอยู่ตอนนี้แล้ว ทั้งสองช่องโหว่นี้ใช้ร่วมกันเพื่อติดตั้งเว็บเชลล์ Chinese Chopper บนเซิร์ฟเวอร์เป้าหมายเพื่อแอบฝังตัวเองและจารกรรมข้อมูล โดยพบการใช้เพื่อแพร่กระจายตัวเองบนเครือข่ายเหยื่ออย่างน้อยตั้งแต่กันยายน 2022 ที่ผ่านมา ซึ่งไมโครซอฟท์เองก็ออกมายอมรับว่ามีการโจมตีจริงตั้งแต่ 30 กันยายน โดยกล่าวว่า “รับรู้ถึงการโจมตีในวงจำกัด ที่ใช้ช่องโหว่ทั้งสองรายการนี้ในการเข้าถึงระบบของผู้ใช้” ล่าสุดได้ออกตัวอัปเดตแพตช์อุดช่องโหว่ทั้งสองรายการนี้ ในฐานะส่วนหนึ่งของชุด Patch Tuesday

ข้อมูลจาก : < https://www.enterpriseitpro.net/microsoft-fixes-proxynotshell-exchange-zero-days/ > 19/11/2022

2 VMware แก้ไขช่องโหว่ร้ายแรงสามรายการ สาเหตุร้ายในการทะลุระบบการยืนยันตัวตนได้แล้ว

VMware ปล่อยตัวอัปเดตด้านความปลอดภัยเพื่อแก้ไขช่องโหว่ร้ายแรงสามรายการในโซลูชั่น Workspace ONE Assist ที่เปิดให้ผู้โจมตีจากภายนอกก้าวข้ามการยืนยันตัวตน พร้อมยกระดับสิทธิ์ตัวเองขึ้นเป็นแอดมินได้ Workspace ONE Assist ใช้ทั้งการควบคุมระยะไกล, แชร์หน้าจอ, จัดการไฟล์ระบบ, และรันคำสั่งจากระยะไกล เพื่ออำนวยความสะดวกแก่ฝ่ายซัพพอร์ตและเจ้าหน้าที่ไอทีในการเข้าถึงระยะไกล และแก้ปัญหาอุปกรณ์แบบเรียลไทม์จากหน้าคอนโซล ช่องโหว่ ทั้งหมดนี้ได้แก่รหัส CVE-2022-31685 (ช่องโหว่ข้ามการยืนยันตัวตน) CVE-2022-31686 (ช่องโหว่ในขั้นตอนการยืนยันตัวตน), และ CVE-2022-31687 (ช่องโหว่ในการควบคุมการยืนยันตัวตน) ทั้งหมดนี้ได้คะแนนความร้ายแรงสูงสุดถึง 9.8 เต็ม 10 ตามสเกล CVSS แพตช์ ที่อัปเดตครั้งนี้เป็นเวอร์ชั่นใหม่ Workspace ONE Assist 22.10 (89993)

ข้อมูลจาก : <https://www.enterpriseitpro.net/vmware-fixes-three-critical/ > 18/11/2022

3 แฮกเกอร์รัสเซียใช้แรนซัมแวร์สายพันธุ์ใหม่ Somnia โจมตีหลายองค์กรในยูเครน

หน่วยงานทางด้านความปลอดภัยทางไซเบอร์ของยูเครน (CERT-UA) ประกาศแจ้งเตือนการแพร่กระจายของแรนซัมแวร์สายพันธุ์ใหม่ที่ชื่อว่า Somnia โดยระบุว่าเป็นปฏิบัติการภายใต้ชื่อว่า 'From Russia with Love' (FRwL) โดยกลุ่ม Z-Team หรืออีกชื่อหนึ่งคือ UAC-0118 โดยการฝังมัลแวร์ไว้บนเว็บไซต์ปลอมเพื่อใช้สำหรับขโมยข้อมูล และเพื่อขัดขวางการทำงานขององค์กรต่าง ๆ ในยูเครน โดยกลุ่มแฮ็กเกอร์ได้ใช้เว็บไซต์ปลอมที่เลียนแบบซอฟต์แวร์ "Advanced IP Scanner" เพื่อหลอกให้พนักงานขององค์กรต่าง ๆ ในยูเครนให้ดาวน์โหลดโปรแกรมมาติดตั้ง ซึ่งจริงๆ แล้วโปรแกรมดังกล่าวคือมัลแวร์ Vidar stealer ซึ่งจะถูกใช้เพื่อขโมย Telegram session เพื่อเข้าควบคุมบัญชี Telegram ของเหยื่อ

แนวทางการป้องกัน

- ตรวจสอบแหล่งที่มาของไฟล์ก่อนดาวน์โหลด
- เปิดใช้งาน Multi-Factor Authentication

ข้อมูลจาก : < https://www.i-secure.co.th/2022/11/แฮ็กเกอร์รัสเซียใช้แรน/ > 16/11/2022