วันที่ 22 สิงหาคม 2568

Zoom และ Xerox ออกอัปเดตความปลอดภัยสำคัญเพื่อแก้ไขช่องโหว่ยกระดับสิทธิ์และรันโค้ดจากระยะไกล

ล่าสุด Zoom และ Xerox ได้ออกอัปเดตความปลอดภัยเพื่อแก้ไขช่องโหว่ร้ายแรงที่อาจเปิดทางให้ผู้โจมตียกระดับสิทธิ์หรือรันโค้ดจากระยะไกลได้ ผู้ใช้งานผลิตภัณฑ์ทั้งสองแบรนด์ควรรีบตรวจสอบและอัปเดตโดยด่วน

ช่องโหว่ใน Zoom Clients for Windows

ช่องโหว่ที่กระทบ Zoom Clients for Windows ถูกติดตามในรหัส CVE-2025-49457 (คะแนน CVSS: 9.6) เป็นปัญหาเกี่ยวกับ “การค้นหาเส้นทางที่ไม่ปลอดภัย” (untrusted search path) ที่อาจนำไปสู่การยกระดับสิทธิ์ของผู้โจมตี

Zoom กล่าวว่า “ช่องโหว่การค้นหาเส้นทางที่ไม่ปลอดภัยใน Zoom Clients for Windows บางรุ่น อาจทำให้ผู้ใช้ที่ไม่ได้ยืนยันตัวตนสามารถยกระดับสิทธิ์ผ่านการเข้าถึงทางเครือข่ายได้”

ปัญหานี้ถูกรายงานโดยทีม Offensive Security ของ Zoom เอง และกระทบกับผลิตภัณฑ์ดังนี้:

- Zoom Workplace for Windows ก่อนเวอร์ชัน 6.3.10
- Zoom Workplace VDI for Windows ก่อนเวอร์ชัน 6.3.10 (ยกเว้นเวอร์ชัน 6.1.16 และ 6.2.12)
- Zoom Rooms for Windows ก่อนเวอร์ชัน 6.3.10
- Zoom Rooms Controller for Windows ก่อนเวอร์ชัน 6.3.10
- Zoom Meeting SDK for Windows ก่อนเวอร์ชัน 6.3.10

ช่องโหว่ใน Xerox FreeFlow Core

Xerox ได้แก้ไขช่องโหว่หลายรายการใน FreeFlow Core โดยเฉพาะช่องโหว่ที่ร้ายแรงที่สุดที่อาจนำไปสู่การรันโค้ดจากระยะไกล ปัญหาเหล่านี้ได้รับการแก้ไขแล้วในเวอร์ชัน 8.0.4 และมีดังนี้:

- CVE-2025-8355 (คะแนน CVSS: 7.5): ช่องโหว่ XML External Entity (XXE) injection ที่นำไปสู่การโจมตีแบบ server-side request forgery (SSRF)
- CVE-2025-8356 (คะแนน CVSS: 9.8): ช่องโหว่ path traversal ที่นำไปสู่การรันโค้ดจากระยะไกล

Horizon3.ai บริษัทด้านความปลอดภัยไซเบอร์ระบุว่า “ช่องโหว่เหล่านี้สามารถถูกโจมตีได้ง่ายมาก และหากถูกใช้โจมตี อาจทำให้ผู้ไม่หวังดีสามารถรันคำสั่งใดๆ บนระบบที่ได้รับผลกระทบ ขโมยข้อมูลสำคัญ หรือพยายามเจาะลึกเข้าไปในระบบเครือข่ายองค์กรเพื่อโจมตีต่อได้”

- CVE-2025-8355 เกิดจากไฟล์ไบนารี (“jmfclient.jar”) ที่ใช้ฟังก์ชันการประมวลผล XML โดยไม่ได้กรอง ทำให้ผู้โจมตีสามารถส่งคำขอพิเศษเพื่อทำการโจมตีแบบ SSRF
- CVE-2025-8356 เกิดจากการจัดการคำสั่ง JMF ที่ไม่รัดกุม ทำให้เกิดช่องโหว่ path traversal ซึ่งสามารถใช้วางเว็บเชลล์ ในตำแหน่งที่เข้าถึงได้จากสาธารณะ

นักวิจัยด้านความปลอดภัย Jimi Sebree กล่าวว่า “แม้บริการบนพอร์ต 4004 จะไม่มีฟีเจอร์ที่ให้บริการไฟล์นี้ได้โดยตรง แต่พอร์ทัลเว็บหลักมีฟังก์ชันครบถ้วนสำหรับรันและให้บริการเพย์โหลดอันตรายของเรา”

ข้อมูลอ้างอิง

Aug 13, 2025, By Ravie Lakshmanan

- https://thehackernews.com/2025/08/zoom-and-xerox-release-critical.html