วันที่ 29 พฤษภาคม 2568

ช่องโหว่บน XenServer VM Tools ของ Windows ทำให้ผู้โจมตีสามารถเรียกใช้โค้ดอันตรายได้

Executive Summary

ตรวจพบช่องโหว่ความปลอดภัยใน XenServer VM Tools ที่ได้รับการกำหนดเป็นรหัส CVE-2025-27462, CVE-2025-27463 และ CVE-2025-27464 โดยช่องโหว่เหล่านี้ส่งผลกระทบต่อ XenServer VM Tools สำหรับระบบปฏิบัติการ Windows ทุกเวอร์ชันก่อนเวอร์ชัน 9.4.1 ซึ่งถือเป็นความเสี่ยงด้านความปลอดภัย ช่องโหว่นี้เกิดจากข้อบกพร่องใน Windows Paravirtualization Driver ที่มีการกำหนดสิทธิ์เข้าถึงอุปกรณ์ภายใน VM อย่างไม่ถูกต้อง ทำให้ผู้ใช้งานทั่วไปภายใน VM สามารถเข้าถึงอุปกรณ์ที่ควรจำกัดการเข้าถึงได้ ซึ่งเปิดโอกาสให้ผู้ไม่หวังดีสามารถยกระดับสิทธิ์ (Privilege Escalation) ไปจนถึง ระดับ Kernel-Level Access และอาจนำไปสู่การรันโค้ดที่ไม่ได้รับอนุญาตหรือสร้างความเสียหายต่อระบบ VM ได้

แพลตฟอร์มที่ได้รับผลกระทบ ได้แก่

- Windows VMs บน XenServer 8.4
- Citrix Hypervisor 8.2 CU1 LTSR

ไดรเวอร์ที่มีความเสี่ยง

- PV Bus: เวอร์ชันต่ำกว่า 9.1.11.115
- PV Interface: เวอร์ชันต่ำกว่า 9.1.12.94
- XCP-ng PV Bus (เฉพาะผู้ใช้ XCP-ng): เวอร์ชันต่ำกว่า 9.0.9065

คำแนะนำ (Recommendation)

- ดำเนินการอัปเดต XenServer VM Tools บน Windows VM ทุกเครื่องให้เป็นเวอร์ชั่น 9.4.1 หรือใหม่กว่า
- ดำเนิการตรวจสอบให้แน่ใจว่าได้เปิดการตั้งค่าอนุญาตการอัปเดตไดรเวอร์ I/O อัตโนมัติ หรือไม่
- ดำเนินการตรวจสอบและอัปเดต MCS Catalog หรือ Provisioning Services (PVS) Golden Image เพื่อป้องกันการนำไดรเวอร์เวอร์ชั่นที่มีความเสี่ยงกลับมาใช้งานอีกในขั้นตอนการสร้าง VM ใหม่

ข้อมูลอ้างอิง

- https://gbhackers.com/xenserver-windows-vm-tools-flaw/
- https://cybersecuritynews.com/xenserver-vm-tools-windows-vulnerability/