เอกสารการแจ้งเตือนพบกรณี Ivanti แก้ไขช่องโหว่ระดับ Critical จำนวน 2 รายการ ใน Avalanche (MDM)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ พบกรณี Ivanti ได้ออกแก้ไขช่องโหว่หลายรายการในโซลูชัน Avalanche mobile device management (MDM)[1] ที่รวมถึงช่องโหว่ระดับ Critical จำนวน ๒ รายการ ที่ CVE-2024-24996 และ CVE-2024-29204 ที่สามารถถูก Remote Command Execution ได้ โดยส่งผลกระทบต่อ Avalanche เวอร์ชัน 6.4.2 และต่ำกว่า โดยรายการช่องโหว่ดังนี้[2]

- CVE-2024-24996 (คะแนน CVSS 9.8) เป็นช่องโหว่ Heap Overflow ใน WLAvalancheService component ของ Ivanti Avalanche ที่ทำให้ผู้โจมตีจากระยะไกลที่ไม่ได้รับการรับรองความถูกต้องสามารถ Remote Command Execution ได้
- CVE-2024-29204 (คะแนน CVSS 9.8) เป็นช่องโหว่ Heap Overflow ใน WLAvalancheService component ของ Ivanti Avalanche ที่ทำให้ผู้โจมตีจากระยะไกลที่ไม่ได้ รับการรับรองความถูกต้องสามารถ Remote Command Execution ได้

ทั้งนี้ Ivanti แนะนำผู้ใช้งานและผู้ดูแลระบบให้ดาวน์โหลดตัวติดตั้ง Avalanche และอัปเดตเป็น Avalanche 6.4.3 เวอร์ชันล่าสุด[3] สามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติม ได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

<u>อ้างอิง</u>

1. https://www.ivanti.com/blog/security-update-for-ivanti-avalanche
2. https://www.bleepingcomputer.com/news/security/ivanti-warns-of-critical-flaws-in-its-avalanche-mdm-solution/
3. https://forums.ivanti.com/s/article/Avalanche-6-4-3-Security-Hardening-and-CVEs-addressed?language=en_US