TLP:CLEAR

เอกสารการแจ้งเตือนกรณี Ivanti เตือนช่องโหว่ Connect Secure เกี่ยวกับช่องโหว่ผลิตภัณฑ์ของ Ivanti

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ เกี่ยวกับกรณี Ivanti เตือนช่องโหว่ connect secure เป็นการโจมตีประเภท Stack-Based Buffer Overflow

Ivanti ได้ออกเตือนการโจมตีช่องโหว่ Connect Secure ที่หมายเลข CVE-2025-0282 ซึ่งเป็นช่องโหว่ประเภท Stack-Based Buffer Overflow ที่มีความรุนแรงระดับ Critical (คะแนน CVSS 9.0) โดยช่องโหว่ดังกล่าวเปิดโอกาสให้ผู้โจมตีสามารถดำเนินการจากระยะไกล และติดตั้งมัลแวร์ในระบบได้ [1] ช่องโหว่ดังกล่าวส่งผลกระทบต่อผลิตภัณฑ์ ดังต่อไปนี้

- Ivanti Connect Secure (ก่อนเวอร์ชัน 22.7R2.5)
- Ivanti Policy Secure (ก่อนเวอร์ชัน 22.7R1.2)
- Ivanti Neurons for ZTA Gateways (ก่อนเวอร์ชัน 22.7R2.3)

Ivanti ยืนยันว่าพบการโจมตีเฉพาะใน Ivanti Connect Secure เท่านั้น โดยได้ออกอัปเดตเฟิร์มแวร์เวอร์ชัน 22.7R2.5 เพื่อแก้ไขปัญหาแล้ว ส่วนอัปเดตสำหรับ Policy Secure และ ZTA Gateways จะเผยแพร่ในวันที่ 21 มกราคม 2568 ทั้งนี้ Ivanti รายงานว่าอุปกรณ์ที่ไม่ได้เชื่อมต่อกับอินเทอร์เน็ตนั้น มีความเสี่ยงต่ำ สำหรับผู้ดูแลระบบ Ivanti มีคำแนะนำให้ดำเนินการดังนี้

1. ใช้ Ivanti Integrity Checker Tool (ICT) สแกนหาอุปกรณ์ที่อาจถูกโจมตี
2. หากไม่พบความผิดปกติให้รีเซ็ตอุปกรณ์เป็นค่าโรงงาน ก่อนอัปเดตเป็นเวอร์ชันใหม่
3. หากพบสัญญาณการโจมตี ให้รีเซ็ตเป็นค่าโรงงานเพื่อลบมัลแวร์ จากนั้นติดตั้งเฟิร์มแวร์เวอร์ชันล่าสุด [2]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้และผู้ดูแลระบบผลิตภัณฑ์ที่ได้รับผลกระทบทำการอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบกิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

https://webboard-nsoc.ncsa.or.th/

อ้างอิง

1. https://www.bleepingcomputer.com/news/security/ivanti-warns-of-new-connect-secure-flaw-used-in-zero-day-attacks/
2. https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-0282-CVE-2025-0283?language=en_US

TLP:CLEAR