แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ
- ☒ Financial Damage
- ☒ Reputation Damage
- ☒ Non-compliance
- ☒ Privacy Violation

ผลกระทบต่อระบบ
- ☒ Loss of Confidentiality
- ☒ Loss of Integrity
- ☒ Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือน ช่องโหว่ร้ายแรงของผลิตภัณฑ์ Ivanti (CVE-2025-0282)

วันที่แจ้งเตือน 17 มกราคม 2568

เรียน ผู้บริหารฝ่ายเทคโนโลยีสารสนเทศ ของผู้ประกอบธุรกิจหลักทรัพย์และผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงของผลิตภัณฑ์ Ivanti (CVE-2025-0282) โดยช่องโหว่ดังกล่าวเกิดจากการที่ผู้ไม่หวังดีพยายามทำให้เกิด Stack-Based Buffer Overflow และเขียนทับตำแหน่งหน่วยความจำด้วยโค้ดอันตราย ส่งผลให้ผู้ไม่หวังดีสามารถรันคำสั่งจากระยะไกล (Remote code execution) เข้าสู่ระบบปฏิบัติการของอุปกรณ์ โดยไม่ต้องผ่านการยืนยันตัวตน และสามารถติดตั้งมัลแวรในระบบได้

Ivanti ได้ออกคำแนะนำ เพื่อให้ผู้ใช้งานพิจารณาดำเนินการอัปเดตซอฟตแวรเปนเวอรชันตามที่แนะนำโดยเร็วที่สุด โดยสามารถดาวน์โหลดได้จาก standard download portal ในหน้าเว็บไซต์

Product Name	Affected Version	Solution
Ivanti Connect Secure	22.7R2 through 22.7R2.4	Upgrade เป็น 22.7R2.5
Ivanti Policy Secure	22.7R1 through 22.7R1.2	Patch อาจเผยแพรในวันที่ 21 มกราคม 2568
Ivanti Neurons for ZTA gateways	22.7R2 through 22.7R2.3	Patch อาจเผยแพรในวันที่ 21 มกราคม 2568

นอกจากนี้ Ivanti มีคำแนะนำในการดำเนินการดังนี้

Ivanti Connect Secure:

- ทำการสแกนด้วย Ivanti Integrity Checker Tool (ICT) เพื่อค้นหาอุปกรณ์ที่มีช่องโหว่ดังกล่าว และแนะนำให้รีเซ็ตอุปกรณ์กลับสู่ค่าจากโรงงาน (Factory Reset) เพื่อลบมัลแวร ก่อนที่จะดำเนินการ Upgrade เป็นเวอร์ชัน 22.7R2.5 และเฝ้าระวังอย่างใกล้ชิดโดยการ monitor ผ่านทาง ICT

Ivanti Policy Secure:

- Ivanti รายงานวาอุปกรณที่ไมไดเชื่อมตอกับอินเทอรเน็ตนั้น มีความเสี่ยงต่ำ สำหรับผูดูแลระบบควรตรวจสอบให้แน่ใจเสมอว่าอุปกรณ์ IPS ได้รับการกำหนดค่าให้ตรงตามคำแนะนำของ Ivanti และไม่ได้เชื่อมต่อกับอินเทอรเน็ต ทั้งนี้ ยังไม่มีรายงานการใช้ช่องโหว่ดังกล่าวเพื่อโจมตี Ivanti Policy Secure

Ivanti Neurons for ZTA Gateways:

- กรณี Ivanti Neurons ZTA Gateways อาจยังไม่สามารถถูกโจมตี อย่างไรก็ดี หากผู้ดูแลระบบมีการสร้าง Gateway สำหรับโซลูชันนี้แล้วและไม่ได้มีการเชื่อมต่อกับ ZTA Controller อาจมีความเสี่ยงในการถูกโจมตีบน Gateway ที่ถูกสร้างขึ้น ทั้งนี้ ยังไม่มีรายงานการใช้ช่องโหว่ดังกล่าวเพื่อโจมตี ZTA Gateways

ThaiCERT แนะนำให้หน่วยงานควรเฝ้าระวังและตรวจสอบช่องโหว่ภายในบริษัท และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของบริษัทเป็นประจำสม่ำเสมอ

สำนักงาน ก.ล.ต. และ TCM-CERT เล็งเห็นถึงความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดต่อผู้ประกอบธุรกิจในตลาดทุน จึงขอแจ้งข้อมูลดังกล่าวให้ผู้ประกอบธุรกิจทราบและพิจารณาดำเนินการตามความเหมาะสม เพื่อลดความเสี่ยงและผลกระทบที่อาจจะเกิดขึ้นกับการปฏิบัติงานของบริษัท

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 16 ม.ค. 2568
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
3) https://nvd.nist.gov/vuln/detail/CVE-2025-0282
4) https://www.bleepingcomputer.com/news/security/ivanti-warns-of-new-connect-secure-flaw-used-in-zero-day-attacks/