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

แจ้งเตือนช่องโหว่ร้ายแรงของผลิตภัณฑ์ Ivanti Connect Secure, Ivanti Policy Secure และ Ivanti Neurons for ZTA (CVE-2024-21888 และ CVE-2024-21893)

วันที่แจ้งเตือน 5 กุมภาพันธ์ 2567

ตามที่ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) และ ก.ล.ต. ได้เผยแพร่รายงานช่องโหว่ของผลิตภัณฑ์ Ivanti (CVE-2023-46805 และ CVE-2024-21887) ซึ่งเป็นช่องโหว่ที่มีผลกระทบร้ายแรง ตามรายงานการแจ้งเตือนช่องโหว่ของสำนักงาน ก.ล.ต. เมื่อวันที่ 22 มกราคม 2567 ต่อมา Ivanti ได้ออกคำแนะนำเกี่ยวกับช่องโหว่ใหม่เพิ่มเติมอีก 2 ช่องโหว่ ได้แก่ CVE-2024-21888 และ CVE-2024-21893 โดยมีรายละเอียดดังนี้

1. ช่องโหว่หมายเลข CVE-2024-21888 เป็นช่องโหว่ใน Web Component ของผลิตภัณฑ์ Ivanti Connect Secure และ/หรือผลิตภัณฑ์ Ivanti Policy Secure โดยผู้ไม่หวังดีสามารถใช้ประโยชน์จากช่องโหว่นี้ในการยกระดับสิทธิเพื่อให้ได้รับสิทธิสูงขึ้นเป็นสิทธิระดับผู้ดูแลระบบ (Administrator) บนระบบที่ได้รับผลกระทบ

2. ช่องโหว่หมายเลข CVE-2024-21893 เป็นช่องโหว่ใน SAML Component ของผลิตภัณฑ์ Ivanti Connect Secure, Ivanti Policy Secure และ Ivanti Neurons for ZTA โดยผู้ไม่หวังดีสามารถใช้ประโยชน์จากช่องโหว่นี้เข้าถึงทรัพยากรที่จำกัดบางอย่างได้โดยไม่ต้องผ่านการยืนยันตัวตน ซึ่งส่งผลให้มีซอฟต์แวร์ที่ได้รับผลกระทบดังนี้

1) ผลิตภัณฑ์ Ivanti Connect Secure (ICS) gateway	เวอร์ชั่น 9.x และ เวอร์ชั่น 22.x
2) ผลิตภัณฑ์ Ivanti Policy Secure (ICS) gateway	เวอร์ชั่น 9.x และ เวอร์ชั่น 22.x
3) ผลิตภัณฑ์ Ivanti Neurons for ZTA	เวอร์ชั่น 9.x และ เวอร์ชั่น 22.x

วิธีแก้ไขปัญหาเบื้องต้นสำหรับหน่วยงานที่ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบดังกล่าว ทาง Ivanti ได้ออกคำแนะนำเพื่อลดผลกระทบจากการถูกโจมตี และคำแนะนำเกี่ยวกับวิธีการติดตั้งซอฟต์แวร์แก้ไขช่องโหว่ (Security Patch) โดยสามารถติดตามบทความ และคำแนะนำล่าสุด ได้ที่ https://forums.ivanti.com/s/article/KB-CVE-2023-46805-Authentication-Bypass-CVE-2024-21887-Command-Injection-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US

ทั้งนี้ Ivanti ได้แนะนำให้ทำการรีเซ็ตอุปกรณ์ที่ได้รับผลกระทบเป็นค่าเริ่มต้นจากโรงงานก่อนที่จะทำการติดตั้ง Security Patch เพื่อป้องกันผู้ไม่หวังดีแฝงตัวอยู่บนอุปกรณ์ Ivanti ได้

ข้อมูลอ้างอิง 1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 2 ก.พ. 2567

2) https://nvd.nist.gov/vuln/detail/CVE-2024-21888

3) https://nvd.nist.gov/vuln/detail/CVE-2024-21893