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 และ Ivanti Policy Secure (CVE-2023-46805 และ CVE-2024-21887)

วันที่แจ้งเตือน 22 มกราคม 2567

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) สกมช. และ ศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม (TTC-CERT) ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Connect Secure (ICS) (ชื่อเดิม Pulse Connect Secure) และ Ivanti Policy Secure ที่อาจส่งผลให้ถูกโจมตีเพื่อส่งคำสั่งจากระยะไกล (Remote Code Execution) ทั้งนี้ Ivanti ได้ประกาศแจ้งเตือนช่องโหว่ด้านความปลอดภัยสำหรับผลิตภัณฑ์ Ivanti Connect Secure (ICS) และผลิตภัณฑ์ Ivanti Policy Secure ดังนี้

1. ช่องโหว่หมายเลข CVE-2023-46805 เป็นช่องโหว่ใน Web Component ของผลิตภัณฑ์ Ivanti Connect Secure และ/หรือผลิตภัณฑ์ Ivanti Policy Secure โดยผู้ไม่หวังดีจากระยะไกลสามารถใช้ประโยชน์จากช่องโหว่นี้ เพื่อให้สามารถเข้าถึงระบบโดยหลีกเลี่ยงการตรวจสอบการยืนยันตัวตน (Authentication Bypass)

2. ช่องโหว่หมายเลข CVE-2024-21887 เป็นช่องโหว่ใน Web Component ของผลิตภัณฑ์ Ivanti Connect Secure และ/หรือผลิตภัณฑ์ Ivanti Policy Secure โดยผู้ไม่หวังดีที่ผ่านการยืนยันตัวตน และได้รับสิทธิระดับ Administrator สามารถใช้ประโยชน์จากช่องโหว่นี้ในการโจมตีเพื่อส่งคำสั่งต่าง ๆ (Execute) ที่เป็นอันตรายที่สร้างขึ้นโดยผู้ไม่หวังดีไปยังผลิตภัณฑ์ (Command Injection)

ช่องโหว่ทั้ง 2 นี้ หากนำมาใช้ร่วมกัน อาจทำให้ผู้ไม่หวังดีสามารถโจมตี ควบคุมผลิตภัณฑ์ดังกล่าว และสามารถติดตั้งโปรแกรมต่าง ๆ รวมถึงลบข้อมูล หรือ สร้างบัญชีใหม่พร้อมสิทธิผู้ใช้งานระดับ Administrator ได้

ซอฟต์แวร์ที่ได้รับผลกระทบของผลิตภัณฑ์ Ivanti Connect Secure (ICS) และผลิตภัณฑ์ Ivanti Policy Secure มีดังนี้

1) ผลิตภัณฑ์ Ivanti Connect Secure (ICS) gateway	เวอร์ชั่น 9.x	ทั้งหมดทุกเวอร์ชั่น
2) ผลิตภัณฑ์ Ivanti Connect Secure (ICS) gateway	เวอร์ชั่น 22.x	ทั้งหมดทุกเวอร์ชั่น
3) ผลิตภัณฑ์ Ivanti Policy Secure (ICS) gateway	เวอร์ชั่น 9.x	ทั้งหมดทุกเวอร์ชั่น
4) ผลิตภัณฑ์ Ivanti Policy Secure (ICS) gateway	เวอร์ชั่น 22.x	ทั้งหมดทุกเวอร์ชั่น

ทั้งนี้ ทาง Ivanti ได้ออกคำแนะนำเกี่ยวกับวิธีแก้ไขปัญหาเบื้องต้น สำหรับหน่วยงานที่ใช้งานผลิตภัณฑ์ที่ได้รับผลกระทบดังกล่าว เพื่อลดผลกระทบจากการถูกโจมตี และคำแนะนำเกี่ยวกับวิธีการนำไปใช้ หน่วยงานสามารถดูรายละเอียดเพิ่มเติมได้ที่ 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

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 20 ม.ค. 2567
2) รายการการแจ้งเตือนและข้อแนะนำของศูนย์ประสานงานรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ด้านโทรคมนาคม ประจำวันที่ 18 ม.ค. 2567
3) https://nvd.nist.gov/vuln/detail/CVE-2023-46805
4) https://nvd.nist.gov/vuln/detail/CVE-2024-21887