TLP:CLEAR

เอกสารการแจ้งเตือนกรณีช่องโหว่ร้ายแรงใน Ivanti Cloud Services Appliance

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เกี่ยวกับกรณีช่องโหว่ร้ายแรงใน Ivanti Cloud Services Appliance (CSA) ที่หมายเลข CVE-2024-11639 มีคะแนน (CVSS : 10.0)[1] ที่ทำให้ผู้โจมตีจากระยะไกลสามารถเข้าจัดการสิทธิ์บนอุปกรณ์ Ivanti CSA เวอร์ชัน 5.0.2 หรือต่ำกว่าได้ โดยไม่ต้องมีการยืนยันตัวตนหรือการโต้ตอบจากผู้ใช้ทาง Ivanti แนะนำให้ผู้ดูแลระบบอัปเดตอุปกรณ์ที่ได้รับผลกระทบเป็น CSA เวอร์ชัน 5.0.3 และ Ivanti ยังได้ออกแพตช์เพื่อแก้ไขช่องโหว่ระดับปานกลาง สูง และร้ายแรงในผลิตภัณฑ์อื่น ๆ เช่น Desktop and Server Management (DSM), Connect Secure and Policy Secure, Sentry, และ Patch SDK ช่องโหว่หมายเลข CVE-2024-11639 เป็นช่องโหว่ด้านความปลอดภัยใน CSA ลำดับที่ 6 ที่ได้รับการแก้ไขในช่วงไม่กี่เดือนที่ผ่านมา โดยช่องโหว่ 5 รายการก่อนหน้านี้ที่ได้รับการแก้ไขแล้วมีดังนี้[2]

- CVE-2024-8190 (remote code execution)
- CVE-2024-8963 (admin authentication bypass)
- CVE-2024-9379, CVE-2024-9380, CVE-2024-9381 (SQL injection, OS command injection, path traversal)[3]

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้ผู้ใช้งาน และผู้ดูแลระบบของผลิตภัณฑ์ที่ได้รับผลกระทบอัปเดตเป็นเวอร์ชันล่าสุดทันที เพื่อป้องกันการถูกโจมตีและตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยร้ายแรงด้านอื่น ๆ และตรวจสอบ กิจกรรมต่างๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงาน ตามคำแนะนำและสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

1. https://nvd.nist.gov/vuln/detail/CVE-2024-11639
2. https://www.bleepingcomputer.com/news/security/ivanti-warns-of-maximum-severity-csa-auth-bypass-vulnerability/
3. https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Cloud-Services-Application-CSA-CVE-2024-11639-CVE-2024-11772-CVE-2024-11773?language=en_US

TLP:CLEAR