เอกสารการแจ้งเตือนกรณี Ivanti ออกแพตช์เพื่อแก้ไขช่องโหว่ใหม่จำนวน 4 รายการ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ พบกรณี Ivanti ออกแพตช์เพื่อแก้ไขช่องโหว่ใหม่จำนวน 4 รายการใน Connect Secure และ Policy Secure ซึ่งช่องโหว่ดังกล่าวส่งผลกระทบต่อ Connect Secure และ Policy Secure Gateway ที่สามารถถูก code execution และ denial-of-service (DoS) ช่องโหว่นี้ส่งผลกระทบต่อเวอร์ชัน 9.x และ 22.x โดยรายการช่องโหว่ดังนี้[1]

- CVE-2024-21894 มีคะแนน CVSS 8.2 เป็นช่องโหว่ heap overflow ใน IPSec component ของ Ivanti Connect Secure และ Ivanti Policy Secure ที่ช่วยให้ผู้โจมตีที่ไม่ได้รับการรับรองความถูกต้องสามารถส่งคำขอที่สร้างขึ้นเพื่อทำให้บริการขัดข้องและทำให้เกิดการโจมตี DoS หรืออาจถูก execution arbitrary code

- CVE-2024-22052 มีคะแนน CVSS 7.5 เป็นช่องโหว่ null pointer dereference ใน IPSec component ของ Ivanti Connect Secure และ Ivanti Policy Secure ที่อนุญาตให้ผู้โจมตีที่ไม่ได้รับการรับรองความถูกต้องสามารถส่งคำขอที่สร้างขึ้นเพื่อทำให้บริการขัดข้องและทำให้เกิดการโจมตี DoS

- CVE-2024-22053 มีคะแนน CVSS 8.2 ช่องโหว่ heap overflow ใน IPSec component ของ Ivanti Connect Secure และ Ivanti Policy Secure ช่วยให้ผู้โจมตีที่ไม่ได้รับการรับรองความถูกต้องสามารถส่งคำขอที่สร้างขึ้นเพื่อทำให้บริการขัดข้องและทำให้เกิดการโจมตี DoS หรือ read content from memory ในบางเงื่อนไข

- CVE-2024-22023 มีคะแนน CVSS 5.3 XML entity expansion หรือช่องโหว่ XEE ในองค์ประกอบ SAML ของ Ivanti Connect Secure และ Ivanti Policy Secure ช่วยให้ผู้โจมตีที่ไม่ได้รับการรับรองความถูกต้องสามารถส่งคำขอ XML ที่จัดทำขึ้นเป็นพิเศษ เพื่อทำให้ resource exhaustion ส่งผลให้ limited-time DoS

รวมถึงการแก้ไขช่องโหว่ที่สำคัญอีก 1 รายการที่ส่งผลกระทบต่อ Neurons เวอร์ชันสำหรับ ITSM ที่ CVE-2023-46808 มีคะแนน CVSS 9.9 ที่ทำให้ผู้โจมตีระยะไกลสามารถผ่านการรับรองความถูกต้องอาจนำไปใช้ในการ arbitrary file write และ obtain code execution ช่องโหว่ข้างต้นที่กล่าวมาทั้งหมดยังส่งผลต่อเวอร์ชัน 9.17.0, 9.18.0 และ 9.19.0 เวอร์ชันเก่าที่รองรับทั้งหมดด้วย[2]

ทั้งนี้ Ivanti แนะนำให้ผู้ใช้งานติดตั้งเวอร์ชัน 9.17.1, 9.18.1 และ 9.19.1 ที่มีให้ใช้งาน ซึ่งช่วยแก้ไขปัญหาดังกล่าวได้ ทาง Thaicert แนะนำให้หน่วยงานที่ใช้งานผลิตภัณฑ์ดังกล่าวควรเฝ้าระวังและตรวจสอบการทำงานของผลิตภัณฑ์ที่ใช้งานภายในหน่วยงาน เพื่อตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของหน่วยงานตามคำแนะนำข้างต้น และสามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติม ได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

อ้างอิง

1. https://thehackernews.com/2024/04/ivanti-rushes-patches-for-4-new-flaw-in.html
2. https://securityaffairs.com/161465/security/ivanti-code-execution-dos-flaws.html