แจ้งเตือน : ช่องโหว่

Critical

ผลกระทบทางธุรกิจ

- [x] Financial Damage
- [x] Reputation Damage
- [x] Non-compliance
- [x] Privacy Violation

ผลกระทบต่อระบบ

- [x] Loss of Confidentiality
- [x] Loss of Integrity
- [x] Loss of Availability

TLP Color : CLEAR

ผู้รับสามารถเผยแพร่ข้อมูลสู่สาธารณะได้

แจ้งเตือนช่องโหว่ร้ายแรงของผลิตภัณฑ์ Ivanti Connect Secure, Ivanti Policy Secure และ Ivanti Neurons for ITSM (CVE-2024-21894, CVE-2024-22052, CVE-2024-22053, CVE-2024-22023 และ CVE-2023-46808)

วันที่แจ้งเตือน 12 เมษายน 2567

ThaiCERT สกมช. ได้เผยแพร่รายงานช่องโหว่ที่มีผลกระทบร้ายแรงในผลิตภัณฑ์ Ivanti Connect Secure (ICS) (ชื่อเดิม Pulse Connect Secure), Ivanti Policy Secure และ Ivanti Neurons for ITSM รวมจำนวน 5 รายการ โดยมีรายละเอียดดังตาราง

CVE	Description	Affected	Solution
CVE-2024-21894	ช่องโหว่ heap overflow ใน IPSec component ของ ICS และ Ivanti Policy Secure ส่งผลให้ผู้ไม่หวังดีสามารถส่งคำร้องขอที่สร้างขึ้นเป็นพิเศษเข้าสู่ระบบเพื่อทำให้ระบบขัดข้อง (Denial of Services: DoS) หรือ ส่งคำสั่งที่ไม่ได้รับอนุญาต (arbitrary code) เข้าสู่ระบบได้	**Ivanti Connect Secure (9.x, 22.x) และ Ivanti Policy Secure**	**Patch versions:** **ICS:** 22.1R6.2, 22.2R4.2, 22.3R1.2, 22.4R1.2, 22.4R2.4, 22.5R1.3, 22.5R2.4, 22.6R2.3, 9.1R14.6, 9.1R15.4, 9.1R16.4, 9.1R17.4 และ 9.1R18.5 **Ivanti Policy Secure:** 22.4R1.2, 22.5R1.3, 22.6R1.2, 9.1R16.4, 9.1R17.4 และ 9.1R18.5
CVE-2024-22052	ช่องโหว่ null pointer dereference ใน IPSec component ของ ICS และ Ivanti Policy Secure ส่งผลให้ผู้ไม่หวังดีโจมตีระบบ โดยการทำ DoS ได้		
CVE-2024-22053	ช่องโหว่ heap overflow ใน IPSec component ของ ICS และ Ivanti Policy Secure ส่งผลให้ผู้ไม่หวังดีโจมตีระบบ โดยการทำ DoS หรือ สามารถอ่านข้อมูลจากหน่วยความจำได้		
CVE-2024-22023	ช่องโหว่ XML entity expansion (XEE) ใน SAML component ของ ICS และ Ivanti Policy Secure ส่งผลให้ผู้ไม่หวังดีสามารถส่งคำขอ XML ที่จัดทำขึ้นเป็นพิเศษเข้าสู่ระบบเพื่อทำให้ระบบขัดข้องในช่วงระยะเวลาหนึ่งได้ (limited-time DoS)		
CVE-2023-46808	ช่องโหว่บน Ivanti Neurons for ITSM ส่งผลให้ผู้ไม่หวังดีที่เข้าสู่ระบบจากระยะไกลสามารถเขียนไฟล์ไปยังโฟลเดอร์ที่เก็บข้อมูลอ่อนไหวบนเครื่อง ITSM ได้ และสามารถส่งคำสั่งเข้าสู่เว็บแอปพลิเคชันของผู้ใช้งานได้	**Ivanti Neurons for ITSM (2023.3, 2023.2 and 2023.1)**	upgrading to 2023.X

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 11 เม.ย. 2567
2) https://forums.ivanti.com/s/article/New-CVE-2024-21894-Heap-Overflow-CVE-2024-22052-Null-Pointer-Dereference-CVE-2024-22053-Heap-Overflow-and-CVE-2024-22023-XML-entity-expansion-or-XXE-for-Ivanti-Connect-Secure-and-Ivanti-Policy-Secure-Gateways?language=en_US
3) https://forums.ivanti.com/s/article/CVE-2023-46808-Authenticated-Remote-File-Write-for-Ivanti-Neurons-for-ITSM?language=en_US