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 Standalone Sentry (CVE-2023-41724) และ FortiClient EMS (CVE-2023-48788)

วันที่แจ้งเตือน 28 มีนาคม 2567

ThaiCERT สกมช. ได้เผยแพร่รายงานกรณีเจ้าของผลิตภัณฑ์ Ivanti และ Fortinet ออกซอฟต์แวร์แก้ไขช่องโหว่ (Patch) ระดับร้ายแรง และแนะนำให้หน่วยงานพิจารณาแก้ไขเพื่อป้องกันการใช้ประโยชน์จากช่องโหว่ดังกล่าว ดังนี้

1. Ivanti ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันตามที่แนะนำโดยเร็วที่สุด เพื่อแก้ไขช่องโหว่ CVE-2023-41724 โดยสามารถดาวน์โหลดได้ผ่านทาง standard download portal ในหน้าเว็บไซต์

Version	Affected	Solution
Ivanti Standalone Sentry	9.17.0, 9.18.0, 9.19.0 และ เวอร์ชันที่เก่ากว่า	Upgrade เป็น 9.17.1, 9.18.1, 9.19.1 หรือ เวอร์ชันล่าสุด

2. Fortinet ได้ออกคำแนะนำให้ผู้ใช้งานทำการอัปเดตซอฟต์แวร์เป็นเวอร์ชันตามที่แนะนำโดยเร็วที่สุด เพื่อแก้ไขช่องโหว่ CVE-2023-48788 ดังข้อมูลตามตาราง

Version	Affected	Solution
FortiClientEMS 7.2	ตั้งแต่ 7.2.0 ถึง 7.2.2	Upgrade เป็น 7.2.3 หรือ สูงกว่า
FortiClientEMS 7.0	ตั้งแต่ 7.0.1 ถึง 7.0.10	Upgrade เป็น 7.0.11 หรือ สูงกว่า

ThaiCERT แนะนำให้บริษัทควรเฝ้าระวังและตรวจสอบช่องโหว่ภายในบริษัท และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเป็นอันตรายต่อระบบสารสนเทศของบริษัทเป็นประจำสม่ำเสมอ

ข้อมูลอ้างอิง

1) รายงานการแจ้งเตือนของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ประจำวันที่ 28 ก.พ. 2567
2) https://thehackernews.com/2024/03/ivanti-releases-urgent-fix-for-critical.html
3) https://forums.ivanti.com/s/article/CVE-2023-41724-Remote-Code-Execution-for-Ivanti-Standalone-Sentry?language=en_US
4) https://fortiguard.fortinet.com/psirt/FG-IR-24-007
5) https://www.horizon3.ai/attack-research/attack-blogs/cve-2023-48788-fortinet-forticlientems-sql-injection-deep-dive/