TLP:CLEAR

เอกสารการแจ้งเตือนเกี่ยวกับการรักษาความมั่นคงปลอดภัยอุปกรณ์ Internet of Things (IoT)

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารพบการแจ้งเตือนเกี่ยวกับการป้องกันอุปกรณ์ Internet of Things (IoT) เป็นอุปกรณ์ที่มีเซ็นเซอร์ ซอฟต์แวร์ และการเชื่อมต่อแลกเปลี่ยนข้อมูลผ่านทางอินเทอร์เน็ต ซึ่งควรมีมาตรการรักษาความปลอดภัยของอุปกรณ์ IoT

ด้วยปัจจุบันมีการใช้งานอย่างแพร่หลายของอุปกรณ์ IoT ทำให้ตกเป็นเป้าหมายจากผู้โจมตี ซึ่งอุปกรณ์ IoT จะเก็บรวบรวมข้อมูลจำนวนมากเกี่ยวกับผู้ใช้งานข้อมูลส่วนบุคคลที่สามารถระบุตัวตนได้ ข้อมูลที่เป็นความลับ และข้อมูลที่ละเอียดอ่อน ดังนั้นจึงมีความสำคัญอย่างยิ่งที่จะต้องรักษาความปลอดภัยของอุปกรณ์ IoT และเพื่อปกป้องข้อมูลที่ละเอียดอ่อนที่มีการเก็บรวบรวมหรือบันทึกไว้ อาจมีการรั่วไหลของข้อมูลออกไป จึงควรมีการตรวจสอบช่องโหว่ของ อุปกรณ์ IoTช่องโหว่ของอุปกรณ์ IoT อาจจะมีดังต่อไปนี้

- Default and Weak Passwords
- Insecure Network Services
- Insecure Interfaces
- Outdated Firmware and Software
- Insecure Data Protection
- Inadequate Physical Security

การแก้ไขเบื้องต้นแนะนำให้ผู้ใช้งานและผู้ดูแลระบบพิจารณาตามมาตรการต่อไปนี้

- Use Strong Passphrases and Multi-Factor Authentication (MFA)
- Update Firmware and Software Regularly
- Assess Device Operations
- Buy Products from Reputable Manufacturers
- Implement Physical Access Control Measures

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) แนะนำให้หน่วยงานที่ใช้งานผลิตภัณฑ์ดังกล่าวที่ได้รับผลกระทบควรทำการตามคำแนะนำเบื้องต้น เพื่อป้องกันการถูกโจมตี และควรตรวจสอบการเข้าถึงโดยไม่ได้รับอนุญาตรวมถึงเหตุการณ์ด้านความปลอดภัยที่ร้ายแรง สามารถติดตามข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ https://webboard-nsoc.ncsa.or.th/ หรือ Scan QR Code

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

อ้างอิง

https://www.csa.gov.sg/alerts-advisories/Advisories/2024/ad-2024-012

TLP:CLEAR