

เอกสารการแจ้งเตือนกรณีเตือนถึงช่องโหว่ที่ส่งผลกระทบต่ออุปกรณ์ IoT

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ได้ติดตามสถานการณ์ข้อมูลข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์ จากแหล่งข่าวที่น่าเชื่อถือเกี่ยวกับช่องโหว่ CVE-2020-15858^[1] ซึ่งเป็นช่องโหว่ที่ส่งผลกระทบต่ออุปกรณ์ IoT ที่มีการใช้งานอย่างแพร่หลาย โดยผู้โจมตีสามารถใช้ประโยชน์จากช่องโหว่เพื่อเข้าควบคุมอุปกรณ์ได้จากระยะไกล

โดยช่องโหว่ CVE-2020-15858 เป็นช่องโหว่ของโมดูล EHS8 ใน Cinterion ซึ่งเป็นอุปกรณ์อิเล็กทรอนิกส์ขนาดเล็กที่ติดตั้งอยู่ในอุปกรณ์ IoT โดยโมดูลนี้ช่วยให้อุปกรณ์ IoT สามารถรับ - ส่งข้อมูลกับเครือข่ายด้วยการเชื่อมต่อแบบไร้สาย และจากการทดสอบของนักวิจัยยังพบว่าช่องโหว่ดังกล่าวยังส่งผลกระทบต่อผลิตภัณฑ์ประเภทเดียวกันของ Cinterion ในโมเดลอื่น เช่น BGS5, EHS5 5/6/8, PDS 5/6/8, ELS61, ELS81 และ PLS62

ทั้งนี้ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) ขอแนะนำให้หน่วยงานที่มีการใช้งานอุปกรณ์ IoT ดังกล่าวอยู่ ควรมีการเฝ้าระวังพร้อมกับการตรวจสอบการทำงานของอุปกรณ์ และตรวจสอบกิจกรรมต่าง ๆ ที่อาจเกิดจากการใช้ประโยชน์จากช่องโหว่ CVE-2020-15858 ซึ่งจะเป็นอันตรายต่อระบบสารสนเทศในหน่วยงานของท่าน ทั้งนี้ สามารถติดตามคำแนะนำและข่าวสารเกี่ยวกับภัยคุกคามทางไซเบอร์เพิ่มเติมได้ที่ <https://webboard-nsoc.ncsa.or.th/> หรือ Scan QR Code



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

อ้างอิง

1. <https://www.cve.org/CVERecord?id=CVE-2020-15858>