ประจำวันพุธที่ 22 มิถุนายน 2565

CISA แจ้งเตือนช่องโหว่ร้ายแรง ในอุปกรณ์อุตสาหกรรม โครงสร้างพื้นฐาน

มีการพบช่องโหว่มากถึง 56 รายการ ซึ่งบางรายการถือว่ามีความสำคัญ ในระบบเทคโนโลยีปฏิบัติการทางอุตสาหกรรม (OT) จากผู้ผลิตระดับโลก 10 ราย อาทิเช่น Honeywell, Ericsson, Motorola และ Siemens เป็นต้น ทำให้มีอุปกรณ์มากกว่า 30,000 เครื่องทั่วโลก ตกอยู่ในความเสี่ยง ตามรายงานของ CISA รัฐบาลสหรัฐฯ และนักวิจัยด้านความปลอดภัย

โดยช่องโหว่เหล่านี้ บางส่วนได้รับคะแนนความรุนแรงของ CVSS สูงถึง 9.8 จาก 10 ซึ่งถือว่ามีความเสี่ยงสูงมาก เมื่อพิจารณาว่าอุปกรณ์เหล่านี้ถูกใช้ในระบบโครงสร้างพื้นฐานที่สำคัญ ทั้งในด้านน้ำมัน ก๊าซ เคมี นิวเคลียร์ การผลิตและการจ่ายพลังงาน การผลิต การบำบัดน้ำและการจ่ายน้ำ อุตสาหกรรมเหมือง อาคารและระบบอัตโนมัติต่างๆ ซึ่งช่องโหว่ด้านความปลอดภัยที่ร้ายแรงที่สุด ได้แก่ การเรียกใช้โค้ดจากระยะไกล (RCE) และช่องโหว่ของเฟิร์มแวร์ หากถูกโจมตี อาจทำให้คนร้ายสามารถทำการปิดระบบไฟฟ้าและการส่งจ่ายน้ำ ขัดขวางการจัดหาอาหาร เปลี่ยนอัตราส่วนของส่วนผสมเพื่อทำให้เกิดส่วนผสมที่เป็นพิษได้

โดยช่องโหว่ส่วนใหญ่เกิดขึ้นในอุปกรณ์ OT ระดับ 1 และระดับ 2 ซึ่งอุปกรณ์ระดับ 1 เช่น Programmable Logic Controller (PLC) และ Remote Terminal Unit (RTU) จะควบคุมกระบวนการทางกายภาพ ในขณะที่อุปกรณ์ระดับ 2 จะประกอบด้วยการควบคุมดูแลและการเก็บข้อมูล (SCADA) และระบบอินเทอร์เฟซระหว่างมนุษย์กับเครื่องจักร

นักวิจัยตั้งข้อสังเกตว่าการแก้ไขปัญหาด้านความปลอดภัยเหล่านี้ไม่ใช่เรื่องง่าย เนื่องจากปัญหาเหล่านี้เป็นผลมาจากการออกแบบผลิตภัณฑ์ OT ที่ไม่ปลอดภัย หรือเนื่องจากต้องมีการเปลี่ยนแปลงเฟิร์มแวร์ของอุปกรณ์และโปรโตคอลที่รองรับ “ตามความเป็นจริง กระบวนการนั้นจะใช้เวลานานมาก” อย่างไรก็ตาม พวกเขาได้แนะนำให้ลูกค้าปฏิบัติตามคำแนะนำด้านความปลอดภัยของผู้จำหน่ายแต่ละราย

ที่มาของข่าว : https://www.theregister.com/2022/06/21/56_vulnerabilities_critical_industrial/