แคสเปอร์สกี้ แลป พบช่องโหว่วิกฤตในโปรโตคอลยอดนิยมที่ในวงการอุตสาหกรรม กระเทือนโปรดักส์จากหลายเวนเดอร์

Kaspersky Lab ICS CERT ได้ทำการวิเคราะห์โปรโตคอล OPC UA (Object Linking and Embedding for Process Control Unified Automation) ออกแบบเพื่อปกป้องการโอนถ่ายข้อมูลระหว่างเซิร์ฟเวอร์และไคลเอนท์ในระบบอุตสาหกรรม รวมทั้งโครงสร้างระบบที่มีความสำคัญ การวิเคราะห์พบช่องโหว่ซีโร่เดย์ 17 รายการ ช่วงการติดตั้งโปรโตคอล นำไปสู่ภัยการโจมตีแบบ denial-of-service และ remote code execution ยิ่งไปกว่านั้น ยังพบจุดบกพร่องอีกหลายจุดในโปรดักส์ในตลาดที่สร้างบนโปรโตคอลนี้ ช่องโหว่ทั้งหมดถูกรายงานต่อไปยังผู้พัฒนาซอฟต์แวร์และได้รับการแก้ไขแล้ว

OPC UA เป็นโปรโตคอลสำหรับใช้ในวงการอุตสาหกรรม พัฒนาและเปิดตัวโดย OPC Foundation เมื่อปี 2006 เพื่อความปลอดภัยในการโอนย้ายถ่ายข้อมูลระหว่างระบบต่างๆ ที่อยู่บนเน็ตเวิร์กของวงการธุรกิจอุตสาหกรรม โปรโตคอลนี้เป็นที่ยอมรับใช้กันแพร่หลายในหมู่เวนเดอร์หลักที่จัดจำหน่ายอุปกรณ์ต่างๆ สำหรับรองรับการใช้งานในวงการอุตสาหกรรมรุ่นใหม่ เช่น อุตสาหกรรมการผลิต น้ำมันและก๊าซ ยาและเวชภัณฑ์ เป็นต้น เอ็นเทอร์ไพรซ์ในแวดวงธุรกิจอุตสาหกรรมนี้ ล้วนติดตั้งเกตเวย์ตามโปรโตคอลนี้เพื่อให้การสื่อสารของ automated process control and telemetry กับระบบการควบคุมเฝ้าระวังทางไกล มีความลื่นไหล เพราะสามารถทำการผนวกกระบวนการบริหารจัดการต่างๆ ทั้งหมดไว้ด้วยกันได้เป็นหนึ่งเดียว และยังมีการนำโปรโตคอลนี้มาใช้ในคอมโพเน้นท์ของ IIoT และสมาร์ทซิตี้อีกด้วย ทำให้ผู้ร้ายไซเบอร์ให้ความสนใจเป็นอย่างยิ่ง

ผู้เชี่ยวชาญ Kaspersky Lab ICS CERT ได้ทำการวิเคราะห์สถาปัตยกรรมของ OPC UA รวมไปถึงโปรดักส์ที่อิงโปรโตคอลนี้ โดยทำการตรวจสอบโอเพ่นซอร์สโค้ด (มีใน GitHub) และได้พบข้อผิดพลาดในการออกแบบและการเขียนโค้ดของโปรโตคอล ซึ่งเป็นข้อผิดพลาดที่ไม่ควรมีอยู่เลยในซอฟต์แวร์โครงสร้างที่มีความอ่อนไหวและสำคัญอย่างยิ่ง ซ้ำยังติดตั้งใช้งานกันอยู่แพร่หลายเช่นนี้ ข้อผิดพลาดที่พบ ได้แก่ ช่องโหว่ซีโร่เดย์ถึง 17 จุดใน โปรดักส์ของ OPC Foundation จึงได้รายงานไปยังผู้พัฒนาซอฟต์แวร์ ซึ่งก็ได้ดำเนินการแก้ไขตามที่รายงานไปนั้นเป็นที่เรียบร้อยแล้ว

นอกจากนี้ Kaspersky Lab ICS CERT ได้วิเคราะห์เธิร์ดปาร์ตี้ซอฟต์แวร์ที่อิงโปรโตคอลนี้ เช่น โซลูชั่นจากเวน

เดอร์ชั้นนำหลายแห่ง ส่วนมาก พบว่ามีข้อบกพร่องอันเกิดจากผู้พัฒนาซอฟต์แวร์ไม่ได้ใช้ฟังก์ชั่นการติดตั้งโปรโตคอลบางตัวอย่างถูกต้อง บางกรณี ช่องโหว่ที่มีอยู่ก็มาจากการปรับเสริมอย่างไม่ถูกต้อง ลงบนโครงสร้างของโปรโตคอลนั่นเอง ผู้เชี่ยวชาญได้ค้นพบการติดตั้งฟังก์ชั่นลงบนคอมเมอร์เชียลโปรดักส์เพื่อวางตลาด อย่างไม่ปลอดภัย ถึงแม้ว่าการติดตั้งดั้งเดิมของ OPC Foundation จะไม่มีข้อผิดพลาดมาก็ตาม ผลก็คือ การปรับแต่เสริม (modifications) ที่กระทำไปโดยเวนเดอร์โดยไม่ทราบสาเหตุจูงใจ ลงในลอจิกของโปรโตคอลเช่นนั้น นำมาซึ่งฟังก์ชั่นการใช้งานที่มีความเสี่ยง

ช่องโหว่ที่พบในการติดตั้งโปรโตคอล OPC UA ที่กล่าวมานั้น อาจนำมาซึ่งความเสียหายใหญ่หลวงต่อวงการอุตสาหกรรม เช่น ความเสี่ยงการโจมตีแบบ denial-of-service (DoS) ภัยคุกคามที่น่าประหวั่นพรั่นพรึงต่อระบบอุตสาหกรรมเพราะอาจเข้ามาทำลายล้างหรือปิดกระบวนการทำงานของทั้งระบบเลยก็เป็นได้ หรือ ความเสี่ยงต่อการเข้ามาทำ remote code execution จากทางไกล ผู้ร้ายไซเบอร์สามารถแทรกส่งเซิร์ฟเวอร์คอมมานด์เพื่อเข้ายึดครองควบคุมกระบวนการทำงานของระบบหรือจะรุกล้ำเจาะเข้าไปในเน็ตเวิร์กก็เป็นได้

เซอร์เจย์ เทมนิคอฟ นักวิจัยระบบความปลอดภัยอาวุโส แคสเปอร์สกี้ แลป (Kaspersky lab ICS CERT) กล่าวว่า “บ่อยครั้งที่ผู้พัฒนาซอฟต์แวร์วางใจในเสถียรภาพความปลอดภัยของโปรโตคอลอุตสาหกรรมมากเกินไป และติดตั้งลงในโซลูชั่นของตนโดยไม่ตรวจสอบความปลอดภัยของโปรดักส์โค้ดให้ดีเสียก่อน ช่องโหว่เช่นนี้สามารถสร้างความเสียหายสะเทือนวงการ และกระทบทั้งโปรดักส์ไลน์ได้ทีเดียว ดังนั้น จึงเป็นเรื่องสำคัญอย่างยิ่งที่เวนเดอร์จะต้องใส่ใจกับ เทคโนโลยีที่ใช้กันแพร่หลายเหล่านี้ และม่ควรหลงไปกับความคิดว่าตนสามารถออกแบบสร้างซอฟต์แวร์ขึ้นมาได้เอง หลายคนคิดว่าจะมีประสิทธิภาพ และปลอดภัยมากกว่า ซอฟต์แวร์ที่มีอยู่ แต่ความจริงก็คือ แม้แต่ซอฟต์แวร์ที่ออกแบบมาใหม่ล่าสุดก็ยังอาจมีช่องโหว่อยู่ได้หลายจุดด้วยกัน”

ข้อแนะนำที่ควรปฏิบัติจากแคสเปอร์สกี้ แลป:
• ใส่ใจเรื่องการตรวจสอบความปลอดภัยและทดสอบ ซึ่งให้ถือว่าเป็นกระบวนการที่จำเป็นต้องกระทำในช่วงระหว่างการพัฒนาแอพพลิเคชั่น และห้ามไว้วางใจโปรโตคอล
• ทำการตรวจสอบความถูกต้องเรียบร้อย (audits) และตรวจสอบช่องโหว่ ทดสอบเจาะระบบ(pen testing) เพื่อให้พบช่องโหว่ต่างๆ ที่อาจมีอยู่
• แยกเดี่ยวกระบวนการพัฒนาซอฟต์แวร์ ดังนั้น หากเกิดการเจาะเข้าแอพพลิเคชั่นขึ้นมา ผู้ร้ายก็ไม่มีช่องทางที่จะเจาะเข้าเน็ตเวิร์กได้

อ่านรายงานการวิเคราะห์ความปลอดภัย OPC UA ได้ที่ เว็บไซต์ ของ Kaspersky Lab ICS CERT
https://ics-cert.kaspersky.com/reports/2018/05/10/opc-ua-security-analysis/