แคสเปอร์สกี้ แลป พบช่องโหว่ของตัวชาร์จรถไฟฟ้าที่สามารถสร้างความเสียหายต่อเน็ตเวิร์กบ้านได้

โดยปกติแล้วจะมีการทดสอบช่องโหว่ต่างๆ ของยานยนต์ไฟฟ้ารุ่นใหม่ๆ อยู่เสมอ แต่อุปกรณ์เสริมที่จำเป็นกลับถูกละเลยอยู่บ่อยครั้ง เช่น ตัวชาร์จแบตเตอรี่ เป็นต้น ผู้เชี่ยวชาญของแคสเปอร์สกี้ แลป พบว่า ตัวชาร์จยานยนต์ไฟฟ้าของเวนเดอร์รายใหญ่รายหนึ่งมีช่องโหว่ที่จะทำให้ถูกโจมตีทางไซเบอร์ได้ และการโจมตีที่ประสบความสำเร็จอาจหมายถึงความเสียหายของระบบไฟฟ้าของทั้งบ้าน

ยานยนต์ไฟฟ้าเป็นหัวข้อที่ได้รับความสนใจอย่างมากในปัจจุบันเนื่องจากจะช่วยรักษาสภาพแวดล้อมได้อย่างยั่งยืน ในบางภูมิภาคจะพบเห็นจุดบริการชาร์จไฟทั้งของสาธารณะและเอกชนอยู่ทั่วไป ความนิยมที่เพิ่มขึ้นนี้ทำให้ผู้เชี่ยวชาญของแคสเปอร์สกี้ แลป ตรวจสอบตัวชาร์จสำหรับใช้ภายในบ้านรวมถึงฟีเจอร์การเข้าถึงระยะไกล (remote access) ผู้เชี่ยวชาญพบว่า ตัวชาร์จที่เชื่อมต่อหากถูกรุกล้ำก็สามารถทำให้ไฟฟ้าทำงานเกินกำลัง ทำให้ระบบที่เชื่อมต่ออยู่ล่ม และอาจทำให้ดีไวซ์อื่นๆ ในระบบเสียหายได้

นักวิจัยตรวจพบช่องทางในการใช้คำสั่งบนตัวชาร์จทั้งคำสั่งหยุดขั้นตอนการชาร์จและการตั้งค่ากระแสไฟสูงสุด การหยุดชาร์จนั้นจะเป็นการสกัดกั้นไม่ให้เจ้าของใช้ยานยนต์ไฟฟ้าของตนได้ ส่วนการตั้งค่ากระแสไฟนั้นอาจทำให้มีความร้อนสูงเกิน อุปกรณ์ที่ไม่มีฟิวส์ป้องกันจะเสียหายได้ หาผู้โจมตีต้องการเปลี่ยนค่ากระแสไฟฟ้า ก็จะเข้าเน็ตเวิร์กผ่านวายฟายที่ตัวชาร์จเชื่อมต่ออยู่ และเมื่อดีไวซ์ต่างๆ นั้นเป็นดีไวซ์ที่ใช้งานภายในบ้าน การรักษาความปลอดภัยสำหรับเน็ตเวิร์กไร้สายจึงมีข้อจำกัด ทำให้ผู้โจมตีเข้าควบคุมได้ง่าย เช่นการใช้วิธีเดาสุ่มพาสเวิร์ดซึ่งเป็นวิธีทั่วๆ ไป จากสถิติของแคสเปอร์สกี้ แลป พบว่า การโจมตี IoT ในปี 2018 จำนวน 94% มาจากการสุ่มพาสเวิร์ดแบบ Telnet และ SSH เมื่อผู้โจมตีเข้าถึงเน็ตเวิร์กไร้สายได้แล้ว ก็จะสามารถหาไอพีแอดเดรสของตัวชาร์จได้ง่าย ขั้นต่อไปคือการเริ่มหาประโยชน์จากช่องโหว่และการขัดขวางการทำงานต่างๆ

นักวิจัยได้แจ้งเรื่องช่องโหว่ที่ตรวจพบทั้งหมดไปยังผู้ประกอบการและได้รับการแพทช์แก้ไขเรียบร้อยแล้ว

นายดิมิทรี สกลียาร์ นักวิจัยด้านความปลอดภัยของแคสเปอร์สกี้ แลป กล่าวว่า “คนทั่วไปมักลืมว่าในการโจมตีแบบมีเป้าหมายนั้น โจรไซเบอร์จะมองหาส่วนประกอบเล็กๆ ที่ไม่สะดุดตาเพื่อใช้เป็นช่องทางบุกรุก ดังนั้นเราจึงจำเป็นต้องมองหาช่องโหว่ทั้งในนวัตกรรมและในอุปกรณ์เสริมต่างๆ ด้วย ผู้ประกอบการเองก็ควรระมัดระวังเรื่องดีไวซ์ยานยนต์ และจัดตั้งโครงการล่าบั๊ก หรือสอบถามจากผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์ ในกรณีนี้ เราโชคดีที่แจ้งช่องโหว่ไปยังผู้ประกอบการแล้วได้รับการตอบรับเชิงบวกและรีบแก้ไขอย่างรวดเร็ว ซึ่งช่วยป้องกันการโจมตีที่

อาจเกิดขึ้นได้”

แคสเปอร์สกี้ แลป ขอแนะนำให้ปฏิบัติตามมาตรการด้านความปลอดภัยดังนี้:

• อัพเดทสมาร์ทดีไวซ์ทั้งหมดเป็นเวอร์ชั่นล่าสุดอย่างสม่ำเสมอ ในอัพเดทนั้นอาจจะมีแพทช์สำหรับช่องโหว่ร้ายแรง ซึ่งถ้าละเลยไม่แพทช์ ก็อาจช่วยให้โจรไซเบอร์เข้าถึงระบบในบ้านและชีวิตส่วนตัวได้
• อย่าใช้พาสเวิร์ดที่ตั้งมาเบื้องต้นสำหรับเราเตอร์วายฟายและดีไวซ์อื่นๆ ควรเปลี่ยนเป็นพาสเวิร์ดที่แข็งแกร่ง และไม่ใช้พาสเวิร์ดซ้ำกันในดีไวซ์อื่นๆ
• แนะนำให้แยกเน็ตเวิร์กสมาร์ทโฮมออกจากเน็ตเวิร์กที่ใช้กับดีไวซ์ส่วนตัวของสมาชิกในครอบครัว เพื่อเป็นการป้องกันการติดมัลแวร์จากฟิชชิ่งอีเมล

ท่านสามารถอ่านรายงานฉบับเต็มได้ที่

> Remotely controlled EV home chargers – the threats and vulnerabilities

ข้อมูลสถิติของแคสเปอร์สกี้ แลป เรื่อง IoT

> New trends in the world of IoT threats