ประจำวันจันทร์ที่ 13 มิถุนายน 2565

ช่องโหว่ใน HID Mercury Access Controllers ทำให้แฮกเกอร์สามารถปลดล็อกได้

ผลิตภัณฑ์ที่ใช้ควบคุมการเข้าใช้ที่ใช้ตัวควบคุม HID Mercury ได้รับผลกระทบจากช่องโหว่ร้ายแรงโดยที่แฮ็กเกอร์ใช้เพื่อปลดล็อกจากระยะไกลได้ ช่องโหว่ดังกล่าวถูกค้นพบโดยนักวิจัยของบริษัท XDR Trellix ซึ่งเปิดตัวเมื่อต้นปีนี้หลังจากการควบรวมกิจการของ McAfee Enterprise และ FireEye

ปัญหาในผลิตภัณฑ์จาก LenelS2 ซึ่งเป็น บริษัท ย่อยของผู้ให้บริการยักษ์ใหญ่ด้าน HVAC ที่เชี่ยวชาญด้านโซลูชั่นความปลอดภัยทางกายภาพ แต่ Trellix กล่าวว่าได้รับการยืนยันจาก HID Global ว่าพันธมิตร OEM ทั้งหมดที่ใช้ตัวควบคุมฮาร์ดแวร์บางตัวได้รับผลกระทบ

นักวิจัยของ Trellix แจ้งว่ามีช่องโหว่ทั้งหมด 8 ช่องโหว่ โดยมีถึง 7 รายการได้รับการจัดอันดับระดับความรุนแรง “วิกฤต” ซึ่งช่องโหว่เหล่านี้สามารถใช้ประโยชน์จากการเรียกใช้โค้ดจากระยะไกล การแทรกคำสั่ง การปฏิเสธบริการ (DoS) การปลอมแปลงข้อมูล และการเขียนไฟล์โดยพลการ ช่องโหว่เหล่านี้ส่วนใหญ่สามารถถูกโจมตีได้โดยไม่มีการรับรองความถูกต้อง แต่การหาประโยชน์นั้นต้องการการเชื่อมต่อโดยตรงกับระบบเป้าหมาย โดย Sam Quinn เป็นนักวิจัยด้านความปลอดภัยอาวุโสของ Trellix บอกกับSecurityWeek ว่าระบบเหล่านี้ไม่ควรถูกเปิดเผยต่ออินเทอร์เน็ต

ผู้ให้บริการได้ออกคำแนะนำเพื่อแจ้งลูกค้าเกี่ยวกับความพร้อมใช้งานของแพตช์ (อัพเดตเฟิร์มแวร์) และลดผลกระทบ สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐอเมริกา (CISA) ได้เผยแพร่คำแนะนำเพื่อแจ้งองค์กรเกี่ยวกับความเสี่ยงที่เกิดจากช่องโหว่ดังกล่าว

ที่มาของข่าว : https://www.securityweek.com/vulnerabilities-hid-mercury-access-controllers-allow-hackers-unlock-doors