ประจำวันพฤหัสบดีที่ 22 กันยายน 2565

พบช่องโหว่ร้ายแรงจากการแฮ็กจากระยะไกลในหน่วยจ่ายไฟของ Dataprobe

สำนักงานความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐานของสหรัฐ (CISA) ได้ออกเตือนด้านระบบควบคุมอุตสาหกรรม (ICS) เกี่ยวกับช่องโหว่ด้านความปลอดภัย 7 รายการในผลิตภัณฑ์หน่วยจ่ายไฟ iBoot-PDU ของ Dataprobe โดยหากใช้ประโยชน์จากช่องโหว่เหล่านี้ได้สำเร็จอาจนำไปสู่การเรียกใช้โค้ดจากระยะไกลโดยไม่ได้รับอนุญาตบนอุปกรณ์ Dataprobe iBoot-PDU

iBoot-PDU เป็นหน่วยจ่ายไฟ (PDU) ที่ให้ผู้ใช้งานสามารถในการตรวจสอบแบบเรียลไทม์และกลไกการแจ้งเตือนที่ซับซ้อนผ่านอินเทอร์เฟซบนเว็บ เพื่อควบคุมการจ่ายไฟให้กับอุปกรณ์ ซึ่งช่องโหว่นี้มีความสำคัญในการเข้าถึง PDU ได้ไม่น้อยกว่า 2,600 ตัวบนอินเทอร์เน็ต โดยอุปกรณ์ Dataprobe เกือบหนึ่งในสามของอุปกรณ์ที่ถูกเปิดเผยตามรายงานปี 2021 จาก Censys และการวิเคราะห์เฟิร์มแวร์ PDU ของ Claroty แสดงให้เห็นว่าผลิตภัณฑ์มีปัญหาการ injection ซึ่งทำให้ลูกค้ามีความเสี่ยงด้านความปลอดภัย

- CVE-2022-3183 (CVSS score: 9.8) – ช่องโหว่ในการ injection คำสั่งที่เกิดจากการไม่ล้างข้อมูลของผู้ใช้
- CVE-2022-3184 (CVSS score: 9.8) – ช่องโหว่การข้ามเส้นทางที่ทำให้สามารถเข้าถึงหน้า PHP ที่ไม่ผ่านการตรวจสอบสิทธิ์ ซึ่งอาจถูกนำไปใช้ในทางที่ผิดเพื่อแทรกโค้ดที่เป็นอันตราย

โดยช่องโหว่ที่ยังไม่ถูกเปิดเผยอีก 5 รายการ (ตั้งแต่ CVE-2022-3185 ถึง CVE-2022-3189) อาจถูกโจมตีโดยผู้ไม่หวังดีเพื่อเข้าถึงหน้าการจัดการหลักของอุปกรณ์จากคลาวด์และสามารถหลอกให้เซิร์ฟเวอร์เชื่อมต่อกับระบบภายในหรือภายนอกตามอำเภอใจ

ผู้ใช้ Dataprobe iBoot-PDU ควรอัปเกรดเป็นเฟิร์มแวร์เวอร์ชันล่าสุด (1.42.06162022) รวมทั้งปิดใช้งาน SNMP, Telnet และ HTTP หากไม่ได้ใช้งาน เพื่อเป็นการป้องกันช่องโหว่เหล่านี้

ที่มาของข่าว : https://thehackernews.com/2022/09/critical-remote-hack-flaws-found-in.html