ประจำวันพุธที่ 27 กรกฎาคม 2565

แฮกเกอร์ใช้ประโยชน์จากช่องโหว่ Zero-Day เพื่อขโมยข้อมูลการชำระเงินจากร้านค้าออนไลน์ PrestaShop

ผู้โจมตีใช้ประโยชน์จากช่องโหว่ในแพลตฟอร์มอีคอมเมิร์ซแบบโอเพนซอร์ส PrestaShop เพื่อใส่โค้ด Skimmer ที่เป็นอันตรายซึ่งออกแบบมาเพื่อรับข้อมูลที่สำคัญ

มีการเผยแพร่เมื่อวันที่ 22 กรกฎาคม ว่าผู้โจมตีพบวิธีการใช้ช่องโหว่ด้านความปลอดภัยเพื่อดำเนินการโค้ดโดยอำเภอใจในเซิร์ฟเวอร์ที่ใช้งานเว็บไซต์ PrestaShop เป้าหมายคือการนำโค้ดที่เป็นอันตรายซึ่งสามารถขโมยข้อมูลการชำระเงินที่ลูกค้าป้อนในหน้าชำระเงิน ซึ่งร้านค้าที่ใช้ซอฟต์แวร์เวอร์ชันเก่าหรือโมดูลของบุคคลที่สามที่มีช่องโหว่ดูเหมือนจะเป็นเป้าหมายหลัก

ผู้ดูแล PrestaShop ยังกล่าวอีกว่าพบช่องโหว่ zero-day ได้รับการแก้ไขแล้วในเวอร์ชัน 1.7.8.7 การแก้ไขความปลอดภัยนี้ช่วยเสริมความแข็งแกร่งให้กับการจัดเก็บแคช MySQL Smarty ต่อการโจมตีด้วย code injection คุณลักษณะเดิมนี้ได้รับการปรับปรุงด้วยเหตุผลด้านความเข้ากันได้และจะถูกลบออกจากเวอร์ชัน PrestaShop ในอนาคต

ปัญหาคือช่องโหว่ของการ injection SQL ได้ส่งผลกระทบในเวอร์ชัน 1.6.0.10 หรือสูงกว่า หมายเลขช่องโหว่ CVE-2022-36408 หากการใช้ประโยชน์จากช่องโหว่ประสบความสำเร็จอาจทำให้ผู้โจมตีสามารถส่งคำขอที่ออกแบบมาเป็นพิเศษซึ่งให้ความสามารถในการดำเนินการตามคำสั่งโดยอำเภอใจ ในกรณีนี้ได้มีให้กรอกแบบฟอร์มการชำระเงินปลอมในหน้าชำระเงินเพื่อรวบรวมข้อมูลบัตรเครดิต การโจมตีของ Magecart พุ่งเป้าไปที่แพลตฟอร์มสั่งอาหารของร้านอาหาร MenuDrive, Harbortouch และ InTouchPOS ซึ่งนำไปสู่การ compromise กับร้านอาหารอย่างน้อย 311 แห่ง

ที่มาของข่าว : https://thehackernews.com/2022/07/hackers-exploit-prestashop-zero-day-to.html