Un grupo de hackers está explotando una vulnerabilidad de seguridad previamente desconocida en la plataforma de comercio electrónico PrestaShop de código abierto, con el fin de inyectar un código de skimmer malicioso diseñado para deslizar información confidencial.

> *«Los atacantes encontraron una forma de utilizar una vulnerabilidad de seguridad para llevar a cabo la ejecución de código arbitrario en servidores que ejecutan sitios web de PrestaShop»*, dijo la compañía el 22 de julio.

PrestaShop se comercializa como la solución de comercio electrónico de código abierto líder en Europa y América Latina, utilizada por casi 300,000 comerciantes en línea en todo el mundo.

El objetivo de las infecciones es introducir un código malicioso capaz de robar la información de pago ingresada por los clientes en las páginas de pago. Las tiendas que utilizan versiones desactualizadas del software u otros módulos vulnerables de terceros parecen ser los principales objetivos.

Los mantenedores de PrestaShop también dijeron que encontraron una falla de día cero en su servicio que dijeron que se solucionó en la versión 1.7.8.7, aunque advirtieron que *«no podemos estar seguros de que sea la única forma en que pueden realizar el ataque».*

> *«Esta solución de seguridad fortalece el almacenamiento en caché de MySQL Smarty contra los ataques de inyección de código. Esta función heredada se mantiene por motivos de compatibilidad con versiones anteriores y se eliminará de futuras versiones de PrestaShop»,* dijo PrestaShop.

El problema en cuestión es una vulnerabilidad de inyección SQL que afecta a las versiones 1.6.0.10 o posteriores, y se rastrea como CVE-2022-36408.

La explotación exitosa de la vulnerabilidad podría permitir que un atacante envíe una solicitud especialmente diseñada que otorga la capacidad de ejecutar instrucciones arbitrarias, en este caso, inyectar un formulario de pago falso en la página de pago para recopilar información de la tarjeta de crédito.

El desarrollo sigue a una ola de ataques de Magecart dirigidos a las plataformas de pedidos de restaurantes MenuDrive, Harbortouch e InTouchPOS, lo que llevó al compromiso de al menos 311 restaurantes.