Los perpetradores han sido identificados aprovechando una vulnerabilidad crítica en Magento para insertar una puerta trasera persistente en páginas de comercio electrónico.

El ataque se sirve de CVE-2024-20720 (evaluado con una puntuación CVSS de 9.1), que ha sido descrito por Adobe como un caso de *«neutralización inadecuada de elementos especiales»* que podría allanar el camino para la ejecución arbitraria de código.

La compañía abordó este problema como parte de las actualizaciones de seguridad lanzadas el 13 de febrero de 2024.

Sansec informó que descubrieron una *«plantilla de diseño ingeniosamente elaborada en la base de datos»* que está siendo utilizada para inyectar automáticamente código malicioso para ejecutar comandos arbitrarios.

> *«Los atacantes combinan el analizador de diseño de Magento con el paquete beberlei/assert (instalado por defecto) para ejecutar comandos del sistema»*, afirmó la compañía.
>
> *«Dado que el bloque de diseño está asociado con el carrito de compras, este comando se ejecuta cada vez que se solicita /checkout/cart».*

El comando en cuestión es *sed*, que se utiliza para insertar una puerta trasera de ejecución de código que luego es responsable de distribuir un skimmer de pagos de Stripe para capturar y extraer información financiera hacia otra tienda Magento comprometida.

Este desarrollo coincide con el gobierno ruso acusando a seis personas de usar malware skimmer para robar información de tarjetas de crédito y pagos de tiendas de comercio electrónico extranjeras, al menos desde finales de 2017.

Los sospechosos son Denis Priymachenko, Alexander Aseyev, Alexander Basov, Dmitry

Kolpakov, Vladislav Patyuk y Anton Tolmachev. Según informó Recorded Future News, los arrestos se llevaron a cabo hace un año, citando documentos judiciales.

> *«Como resultado, los miembros del grupo de hackers adquirieron ilegalmente información sobre casi 160 mil tarjetas de pago de ciudadanos extranjeros, y posteriormente las vendieron a través de sitios clandestinos en internet»*, declaró la Fiscalía General de la Federación Rusa.