Agentes de amenazas están aprovechando activamente una vulnerabilidad crítica recientemente expuesta en el complemento de WordPress *«WooCommerce Payments»* como parte de una amplia campaña dirigida.

La vulnerabilidad, identificada como CVE-2023-28121 (puntuación CVSS: 9.8), es un caso de elusión de autenticación que permite a atacantes no autenticados hacerse pasar por usuarios arbitrarios y llevar a cabo algunas acciones en nombre del usuario suplantado, incluyendo un administrador, lo que podría llevar a la toma de control del sitio.

> *«Los ataques a gran escala contra la vulnerabilidad, asignada como CVE-2023-28121, comenzaron el jueves 14 de julio de 2023 y continuaron durante el fin de semana, alcanzando un máximo de 1.3 millones de ataques contra 157,000 sitios el sábado 16 de julio de 2023»,* dijo el investigador de seguridad de Wordfence, Ram Gall, en una publicación el lunes.

Las versiones 4.8.0 a 5.6.1 de WooCommerce Payments son vulnerables. El complemento está instalado en más de 600,000 sitios. Se lanzaron correcciones para la vulnerabilidad por parte de WooCommerce en marzo de 2023, y WordPress emitió actualizaciones automáticas para los sitios que utilizan versiones afectadas del software.

Un factor común observado en los ataques involucra el uso del encabezado de solicitud HTTP *«X-Wcpay-Platform-Checkout-User: 1»*, lo que provoca que los sitios susceptibles traten cualquier carga adicional como si proviniera de un usuario administrador.

Wordfence indicó que esta vulnerabilidad está siendo utilizada para implementar el complemento «WP Console», que un administrador puede usar para ejecutar código malicioso e instalar un cargador de archivos para establecer persistencia y crear una puerta trasera en el sitio comprometido.

Vulnerabilidades de Adobe ColdFusion aprovechadas en el mundo real

La revelación surge cuando Rapid7 informó que ha detectado la explotación activa de fallos en Adobe ColdFusion en varios entornos de clientes a partir del 13 de julio de 2023, con el propósito de instalar web shells en dispositivos infectados.

«Los actores maliciosos parecen estar aprovechando CVE-2023-29298 junto con otra vulnerabilidad secundaria», mencionó Caitlin Condon, investigadora de seguridad de Rapid7. La falla adicional se identifica como CVE-2023-38203 (puntuación CVSS: 9.8), una vulnerabilidad de deserialización que fue solucionada mediante una actualización extraordinaria lanzada el 14 de julio.

La vulnerabilidad CVE-2023-29298 (puntuación CVSS: 7.5) se refiere a un fallo de omisión de control de acceso que afecta a ColdFusion 2023, ColdFusion 2021 Update 6 y versiones anteriores, y ColdFusion 2018 Update 16 y versiones anteriores.

> *«Esta vulnerabilidad permite a un atacante acceder a los puntos de administración al insertar un carácter de barra diagonal adicional e inesperado en la URL solicitada»,* reveló la empresa Rapid7 la semana pasada.

Sin embargo, Rapid7 advirtió que la solución para CVE-2023-29298 es incompleta y que podría ser modificada fácilmente para evadir los parches lanzados por Adobe.

Se recomienda a los usuarios actualizar a la versión más reciente de Adobe ColdFusion para protegerse contra posibles amenazas, ya que las correcciones implementadas para resolver CVE-2023-38203 interrumpen la cadena de explotación.