Se descubrió que la última versión de la biblioteca OpenSSL es susceptible a una vulnerabilidad de corrupción de memoria remota en sistemas seleccionados.

El problema fue identificado en la versión 3.0.4 de OpenSSL, que se lanzó el 21 de junio de 2022, y afecta a los sistemas x64 con el conjunto de instrucciones AVX-512. OpenSSL 1.1.1, así como las bifurcaciones de OpenSSL, BoringSSL y LibreSSL, no se ven afectadas.

El investigador de seguridad Guido Vrkanken, quien informó sobre el error a fines de mayo, dijo que *«un atacante puede desencadenarlo de forma trivial»*. Aunque se corrigió la vulnerabilidad, aún no hay parches disponibles.

OpenSSL es una biblioteca de criptografía popular que ofrece una implementación de código abierto del protocolo Transport Layer Security (TLS). Advanced Vector Extensions (AVX) son extensiones de la arquitectura del conjunto de instrucciones x86 para microprocesadores de Intel y AMD.

> *«No creo que esta sea una vulnerabilidad de seguridad. Es solo un error grave que hace que la versión 3.0.4 no se pueda usar en máquinas compatibles con AVX-512»,* dijo Tomás Mráz de OpenSSL Foundation.

> Por otro lado, Alex Gaynor dijo: *«No estoy seguro de entender cómo no es una vulnerabilidad de seguridad. Es un desbordamiento de búfer de almacenamiento dinámico que puede activarse mediante cosas como firmas RSA, que pueden ocurrir fácilmente en contextos remotos (por ejemplo, un protocolo de enlace TLS)».*

Xi Ruoyao, estudiante de posgrado en la Universidad de Xidian, intervino y afirmó que aunque *«creo que no deberíamos marcar un error como 'vulnerabilidad de seguridad' a menos que tengamos alguna evidencia que muestre que puede (o al menos puede) ser explotado»,* es necesario lanzar la versión 3.0.5 lo antes posible debido a la gravedad del

problema.