



## Vulnerabilidad crítica detectada en la máquina virtual Move que alimenta la red blockchain de Aptos

Investigadores de seguridad cibernética revelaron detalles sobre una vulnerabilidad crítica ya parcheada en la máquina virtual Move, que alimenta la red blockchain de Aptos.

La vulnerabilidad «*puede hacer que los nodos de Aptos se bloqueen y provoquen la denegación de servicio*», dijo Numen Cyber Labs, con sede en Singapur, en un [artículo técnico](#).

Aptos es un [nuevo participante](#) en el espacio blockchain, que lanzó su [red principal](#) el 17 de octubre de 2022. Tiene sus raíces en el sistema de pago de moneda estable Diem propuesto por Meta, que también introdujo una billetera digital de corta duración llamada Novi.

La red se construye utilizando un lenguaje de programación independiente de la plataforma conocido como [Move](#), un sistema basado en Rust que está [diseñado](#) para implementar y ejecutar contratos inteligentes en un entorno de tiempo de ejecución seguro, también conocido como Move Virtual Machine (MoveVM).

La [vulnerabilidad](#) identificada por Numen Cyber Labs, tiene sus raíces en el módulo de verificación del lenguaje Move («[stack\\_usage\\_verifier.rs](#)»), un componente que valida las instrucciones del código de bytes antes de su ejecución en MoveVM.

Específicamente, se relaciona con una [vulnerabilidad de desbordamiento de enteros](#) en el lenguaje de programación Web3 basado en pilas, que podría provocar un comportamiento indefinido, y por lo tanto, bloqueos.

«*Debido a que esta vulnerabilidad ocurre en el módulo de ejecución de Move, para los nodos de la cadena, si se ejecuta el código bytecode, provocará un ataque [de denegación de servicio]*», explicó la compañía de ciberseguridad.



## Vulnerabilidad crítica detectada en la máquina virtual Move que alimenta la red blockchain de Aptos

«En casos severos, la red de Aptos puede detenerse por completo, lo que causará daños incalculables y tendrá un impacto grave en la estabilidad del nodo».