Hace dos años, en 2018, un investigador de seguridad cibernética descubrió una vulnerabilidad importante en Bitcoin Core, el software que impulsa la cadena de bloques de Bitcoin, pero después de informar sobre el problema y repararlo, el investigador decidió mantener la privacidad de los detalles para evitar que los hackers exploten la falla.

Los detalles técnios de la vulnerabilidad se publicaron a inicios de la semana, luego de descubrirse de forma independiente la misma vulnerabilidad en otra criptomoneda, basada en una versión anterior del código de Bitcoin que no había recibido el parche.

Llamada INVDoS, la vulnerabilidad es un ataque clásico de denegación de servicio (DoS). Aunque en muchos casos los ataques DoS son inofensivos, no lo son para sistemas accesibles a través de Internet, que deben tener un tiempo de actividad estable para procesar transacciones.

INVDoS fue descubierto en 2018 por Braydon Fuller, un ingeniero de protocolo de Bitcoin. Fuller descubrió que un atacante podría crear transacciones de Bitcoin con formato incorrecto que, al ser procesados por los nodos de la cadena de bloques de Bitcoin, conducirían a un consumo descontrolado de los recursos de memoria del servidor, lo que eventualmente colapsaría los sistemas afectados.

> *«En el momento del descubrimiento, esto representaba más del 50% de los nodos de Bitcoin publicitados de forma pública con tráfico entrante, y probablemente la mayoría de los mineros e intercambios»,* dijo Fullero en un documento publicado el miércoles.

Además, INVDoS también impactó más que los nodos (servidores) de Bitcoin que ejecutan el software Bitcoin Core. Los nodos de Bitcoin que ejecutan Bcoin y Btcd también se vieron afectados por el mismo error.

Otras criptomonedas que se construyeron sobre el protocolo Bitcoin original también se vieron afectadas, como Litecoin y Namecoin.

Fuller dijo que el error era peligroso porque podría *«contribuir a la pérdida de fondos o ingresos».*

> *«Esto podría deberse a una pérdida de tiempo de extracción o al gasto de electricidad al cerrar los nodos y retrasar los bloques o hacer que la red se divida temporalmente»*, dijo.
>
> *«También podría ser a través de la interrupción y el retraso de los contratos urgentes o la prohibición de la actividad económica. Eso podría afectar el comercio, los intercambios, los intercambios atómicos, los depósitos en garantía y los canales de pago HTLC de la red relámpago»*, agregó el investigador.

El error INVDoS se informó a todas las partes responsables y se parcheó, en ese momento, con el identificador CVE-2018-17145, que no incluía muchos detalles para no alertar a los atacantes.

Sin embargo, el mismo error fue descubierto durante el verano por Javed Khan, otro ingeniero de protocolo de Bitcoin, mientras buscaba errores en la criptomoneda Decred.

Khan informó del error al programa de recompensas de errores de Decred y finalmente se reveló al mundo el mes pasado.

Los detalles completos sobre toda la vulnerabilidad INVDoS se publicaron a inicios de esta semana, por lo que otras criptomonedas que bifurcaron versiones anteriores de los protocolos de Bitcoin deben verificar si también resultaron afectadas.

> *«No ha habido una explotación conocida de esta vulnerabilidad en la naturaleza»,* dijeron ambos investigadores.