Bug INVDoS di Bitcoin tenuto segreto per due anni

Set 14, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La falla di sicurezza è stata considerata troppo pericolosa per renderne pubblici i dettagli. È emersa adesso perché individuata da un altro ricercatore.

Troppo "sensibile" per essere divulgata nei dettagli anche una volta che l'aggiornamento era disponibile. Stiamo parlando di **INVDoS**, un bug relativo alla gestione della blockchain **Bitcoin** che è stato scoperto nel 2018 da **Braydon Fuller**, un ricercatore specializzato nel settore.

La vulnerabilità, classificata come CVE-2018-17145, ha seguito una sorta di "corsia preferenziale". Nonostante sia stato sviluppato e distribuito un aggiornamento, infatti, nessun dettaglio tecnico è stato reso pubblico come succede abitualmente. **Il rischio che qualcuno la sfruttasse, infatti, è stato considerato troppo elevato.**

INVDoS è una classica vulnerabilità Denial of Service, in grado cioè di bloccare il funzionamento del software in questione. Parlando di Bitcoin, però, l'ipotesi di un malfunzionamento o di una semplice "sospensione" di funzionamento ha potenziali conseguenze che qualcuno definirebbe devastanti. **Di qui una scelta che, tutto sommato, ha delle fondamenta piuttosto solide**.



Prima di tutto perché un blocco delle operazioni in un sistema blockchain rappresenta, di per sé, un problema notevole. In secondo luogo perché un evento del genere potrebbe inserirsi in una strategia più ampia, **per esempio nell'ipotesi in cui un attacco basato sulla vulnerabilità venga messo a segno in un momento particolarmente "sensibile", come quello del lancio di una nuova cripto-valuta**.

Il codice utilizzato da Bitcoin Core, infatti, è stato "riciclato" da altre cripto-valute e individuare tutte le implementazioni della porzione affetta dal bug era tutt'altro che facile.

Cos'è cambiato adesso? Semplice: la stessa falla è stata individuata da un altro ricercatore (**Javed Khan**) che ha invece deciso di utilizzare il classico "protocollo" per la comunicazione dei dettagli riguardanti la vulnerabilità.

Fuller, di conseguenza, ha deciso di pubblicare un report completo (consultabile a questo indirizzo) in cui affronta il tema fornendo tutti i dettagli che fino a oggi aveva tenuto

nascosti.

Insomma: nel settore delle cripto-valute è un momento molto particolare, in cui molti esperti di sicurezza si domandano se i 24 mesi trascorsi siano stati sufficienti per mettere tutti al riparo da potenziali attacchi. La conferma potrà arrivarci solo nelle prossime settimane e il rischio è che di INVDoS si senta parlare ancora.

Condividi l’articolo

Attacchi a tappeto contro i siti di e-commerce Magento I pirati di TeamTNT all’assalto dei container su cloud

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/09/14/bug-invdos-di-bitcoin-tenuto-segreto-per-due-anni/?utm_source=rss&utm_medium=rss&utm_campaign=bug-invdos-di-bitcoin-tenuto-segreto-per-due-anni