

Pasticcio sulle falle di sicurezza per IBM: online 4 zero-day

Apr 24, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

L'azienda ha ignorato per errore la segnalazione di un ricercatore. Ora i dettagli delle falle di sicurezza sono stati pubblicati.

In un primo momento qualcuno ha pensato che dalle parti di **IBM** avessero deciso di sposare la classica scusa usata in passato da altri colossi dell'informatica per sminuire l'impatto di una falla di sicurezza, ricorrendo al mantra "non è una vulnerabilità, è una feature".

In realtà quello che è successo dalle parti di IBM è un classico pasticcio dovuto a una serie di errori di comunicazione, che hanno però portato a una situazione decisamente spinosa. Qualcosa di simile a ciò che è accaduto a **Microsoft** qualche tempo fa.

Protagonista della vicenda è **Pedro Ribeiro**, direttore del settore di ricerca di **Agile Information Security**. Il ricercatore ha individuato una serie di quattro vulnerabilità all'interno di **IBM Data Risk Manager (IDRM)**, un tool che la società mette a disposizione dei suoi utenti per individuare e analizzare eventuali rischi nella gestione dei dati.

Le falle di sicurezza, nel dettaglio, riguarderebbero un sistema per aggirare l'autenticazione, un bug che consente l'iniezione di comandi, la presenza di una password predefinita e una vulnerabilità che consente di forzare il download di un file.

Vulnerabilità decisamente gravi, che se sfruttate (singolarmente o in sequenza) permetterebbero di portare attacchi ai sistemi che usano IDRM.

Quando Ribeiro ha contattato IBM per segnalare le falle (senza peraltro pretendere alcun compenso sulla base del programma bug bounty dell'azienda) si è sentito però rispondere che le vulnerabilità non venivano considerate perché riguardavano un prodotto "opzionale" dedicato al supporto dei sistemi IBM.

Una cantonata clamorosa, che il ricercatore ha sottolineato spiegando che le vulnerabilità in questione posso portare alla compromissione di tutti i sistemi collegati a IDRM.

A fronte della bizzarra risposta dell'azienda, Ribeiro ha però deciso di rendere pubbliche le vulnerabilità, pubblicando anche dei proof of concept per sfruttarle. Solo a questo punto, dalle parti di IBM si sono resi conto dell'errore e si sono attivati per correggere gli zero-day individuati dal ricercatore.

Al momento, gli sviluppatori IBM hanno corretto due delle vulnerabilità e starebbero lavorando a quelle rimanenti.

Condividi l'articolo

Rapporto Cisco: cloud e automazione sono le sfide della security Clamoroso zero-day permette di attaccare iOS attraverso Mail

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/04/24/pasticcio-sulle-falle-di-sicurezza-per-ibm-online-4-zero-day/?utm_source=rss&utm_medium=rss&utm_campaign=pasticcio-sulle-falle-di-sicurezza-per-ibm-online-4-zero-day