Falla critica in VMware: aggiornare di corsa!

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

La vulnerabilità interessa il sistema di gestione centralizzata di VMware e consentirebbe di accedere a tutte le informazioni conservate sui sistemi.

Non accade spesso che una vulnerabilità ottenga un rating di 10 su 10. Quando succese, per gli amministratori IT significa una sola cosa: grossi guai. Se il bug in questione affligge un software diffuso come **VMware**, poi, la situazione può essere senza dubbio definita critica.

La segnalazione, pubblicata dalla stessa azienda con un documento di approfondimento sul suo sito, riguarda un bug (CVE-2020-3952) all'interno di **VMware Directory Service (vmdir)** e può avere conseguenze devastanti. Se sfruttata, infatti, consentirebbe a un pirata informatico di accedere liberamente a tutte le informazioni memorizzate sui sistemi virtuali.

Il componente in quesitone, infatti, fa parte di **vCenter Server**, il sistema di gestione centralizzato di VMware che gestisce, tra le altre cose, i certificati per l'accesso che permettono di controllare in massa tutte le installazioni. Insomma: violare vmdir significa in pratica avere il controllo assoluto.

La falla di sicurezza permette di aggirare il sistema di autenticazione e, secondo gli sviluppatori di VMware, non è possibile correggerla agendo sulle impostazioni del software. L’unica soluzione, in buona sostanza, è applicare la patch.

La parte più problematica, a quanto si capisce, è capire se la propria installazione è vulnerabile o meno all’attacco. Il bug è presente sulle versioni di vCenter Server aggiornate alla versione 6.7 da installazioni precedenti, mentre le “nuove” installazioni (quelle cioè eseguite direttamente con la versione 6.7) sarebbero sicure.

Gli esperti di VMware, in ogni caso, consigliano di verificare i log di sistema per controllare se il bug sia presente ed eseguire l’aggiornamento il prima possibile. Considerata la diffusione del software di virtualizzazione, infatti, l’impatto di un eventuale exploit in grado di sfruttare la vulnerabilità potrebbe essere devastante.

Condividi l’articolo

Ecco DDG: la prima botnet peer to peer

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/04/14/falla-critica-in-vmware-aggiornare-di-corsa/?utm_source=rss&utm_medium=rss&utm_campaign=falla-critica-in-vmware-aggiornare-di-corsa