Rivoluzione GitHub: ecco gli aggiornamenti automatici per i pacchetti

Mag 30, 2019 Marco Schiaffino In evidenza, News, Prodotto, RSS, Scenario, Tecnologia, Vulnerabilità 0

Il nuovo Dependabot permette agli sviluppatori di ricevere un avviso quando è disponibile un update per le "dipendenze" utilizzate nel progetto.

È la classica rivoluzione "nascosta", di cui buona parte dell'opinione pubblica non verrà mai a conoscenza. La nuova funzione proposta da **GitHub**, però, potrebbe avere un impatto davvero significativo in termini di sicurezza su tutto il mondo dell'informatica.

Il sistema automatizzato per gli aggiornamenti di sicurezza **Dependabot** introdotto dal servizio di hosting per i progetti software rappresenta infatti un enorme passo avanti che potrebbe ridurre in maniera decisiva la superficie di attacco a disposizione dei pirati informatici.

Per capirne il potenziale impatto, bisogna partire da una prima considerazione. Nello scenario attuale, qualsiasi sviluppatore lavora, in buona parte, come un assemblatore che utilizza singoli "pacchetti" sviluppati da altri programmatori.

Ogni software, quindi, contiene al suo interno decine di componenti (le cosiddette "dipendenze") a cui sono affidati compiti specifici, che vengono utilizzati anche da altri programmi.

La prima conseguenza di questo sistema è che ogni volta che compare una vulnerabilità in uno dei pacchetti, questa si ripercuote quasi invariabilmente su tutti i progetti che lo utilizzano come dipendenza. **In pratica, una falla di sicurezza in un singolo pacchetto può potenzialmente generare una vulnerabilità in decine di software**.

Il secondo problema, invece, riguarda la filiera di aggiornamento. In una situazione simile, infatti, la catena degli update diventa molto più complicata. Quello che succede, in molti casi, è che quando viene individuata una falla, l'autore realizzi tempestivamente l'aggiornamento che la corregge, ma tutti gli sviluppatori che usano il suo codice non implementino il suo update, o lo facciano con molto ritardo.

Un ritardo che, in molti casi, è anche dovuto a problemi molto pratici, come i dubbi sulla compatibilità della nuova versione nell'impianto generale dei loro software.

Con la nuova funzionalità di GitHub, tutti questi problemi potranno essere risolti. Il nuovo sistema prevede infatti una

procedura in modalità “pull”. Quando è disponibile un aggiornamento di sicurezza per un pacchetto, tutti gli sviluppatori che lo utilizzano nei loro progetti ricevono un alert che gli consente di scaricare l’update.

Non solo: ogni sviluppatore riceve anche tutta la documentazione, compresa una valutazione di compatibilità generata automaticamente grazie a Dependabot, uno strumento sviluppato da una società specializzata che GitHub (dal 2018 controllata da Microsoft) ha acquisito solo una settimana fa.

In definitiva, quello a cui siamo di fronte è una piccola grande rivoluzione che potrebbe avere conseguenze estremamente positive nel prossimo futuro. Incrociamo le dita.

Condividi l’articolo

Attacco massiccio a Docker. I pirati usano Shodan per colpire gli host L’esercito cinese punta ad abbandonare Windows

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/05/30/rivoluzione-github-ecco-gli-aggiornamenti-automatici-per-i-pacchetti/