Ecco come ti rubo i file con un bug di Firefox

Lug 10, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Una vulnerabilità vecchia di 17 anni può essere sfruttata ancora oggi per copiare tutti i file da una cartella e caricarli su un server esterno.

Da un punto di vista tecnico si definisce come un'implementazione errata della **Same Origin Policy (SOP)** ed è una vulnerabilità emersa in **Firefox** la bellezza di 17 anni fa.

Tutto gira intorno al fatto che il browser, oltre che pagine le pagine Web online, può essere utilizzato per aprire file HTML presenti nella memoria del dispositivo. Una funzionalità utile (anche se sempre meno) in qualche caso, ma che espone al rischio che un file malevolo possa avviare azioni nella directory in cui è memorizzato.

Il bug originale, segnalato nel 2002, riguardava la possibilità che un file potesse leggere gli altri dati nella sua stessa cartella e fosse così possibile accedervi. Per dirla tutta, non era un problema solo di Firefox: a esserne interessati erano tutti i browser disponibili in quel periodo, compreso (per chi se lo ricorda) **Netscape**.

Le soluzioni implementate dagli sviluppatori per correggere il bug sono state diverse e dalle parti di Mozilla hanno scelto di impedire ai file HTML di accedere all'elenco (indexing) dei file all'interno della cartella. In questo modo**, un pirata informatico che avesse voluto rubare un file avrebbe dovuto conoscerne posizione e nome**.

Perché non utilizzare soluzioni più drastiche? Perché la lettura via Browser di file HTML ha ancora qualche utilità, per esempio la visualizzazione delle guide software (molti produttori usano ancora HTML) e “troncare” la possibilità di visualizzarli avrebbe creato qualche problema.

La scelta di introdurre una protezione “light”, però, ha lasciato aperta la possibilità di sfruttare la vulnerabilità. Anche se in maniera decisamente elaborata. A segnalarlo agli sviluppatori di Mozilla è stato **Vladimir Bostanov** nel luglio del 2018.

Il ricercatore si è infatti reso conto che con qualche accorgimento (e un generoso uso di ingegneria sociale) è possibile sfruttare il bug anche oggi. La tecnica di attacco prevederebbe l’invio del file malevolo alla vittima che, una volta aperto, mostri un elenco dei file in cartella e un messaggio che chiede di “fare clic per sbloccare il contenuto”**. Il clic sul link potrebbe avviare il JavaScript che trasferirebbe i file della cartella sul server del pirata informatico**.

Complicato? Forse. Plausibile? Sicuramente. Nel passato, tutto sommato, abbiamo visto attacchi avere un discreto successo adottando strategie molto più improbabili.

La vulnerabilità è stata resa pubblica il **16 gennaio 2019**, ma nonostante ciò non è arrivata alcuna patch per correggere la falla.

Qualche giorno fa, però, a riaccendere i riflettori sul problema legato alla gestione della SOP in Firefox ci ha pensato un altro ricercatore, **Barak Tawily**.

Nel suo report, corredato anche da un video, Tawily spiega come sfruttare il bug per sottrarre informazioni dal computer dell'ignara vittima sfruttando la vulnerabilità.

[embedded content]

Ora sembra che dale parti di Mozilla abbiano deciso di prendere delle contromisure più serie e che il problema verrà risolto una volta per tutte. Nel frattempo, il suggerimento è quello di diffidare dei file HTML in download.

Condividi l'articolo

Zero-day nella versione Mac di Zoom. La webcam attivata in remoto

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/10/ecco-come-ti-rubo-i-file-con-un-bug-di-firefox/