Google ha annunciato la rimozione di Entrust come autorità di certificazione (CA) affidabile da Chrome. Questo significa che i siti web che utilizzano certificati Entrust emessi dopo il 31 ottobre 2024 non saranno più considerati sicuri da Chrome.

Fin dai primi tempi dell'informatica, gli scienziati informatici hanno riconosciuto l'importanza del trasporto sicuro delle informazioni. I primi protocolli, come Telnet, trasmettevano dati come nomi utente e password attraverso internet senza crittografia, rendendoli visibili a chiunque volesse intercettarli. Questi protocolli sono stati poi sostituiti da versioni più sicure che utilizzano la crittografia a chiave pubblica, su cui oggi si basano la maggior parte dei siti web per trasferire in modo sicuro le informazioni tra i loro server e il browser degli utenti.

I siti web utilizzano certificati digitali per convalidare la loro identità e fornire chiavi pubbliche di crittografia che il browser può utilizzare per stabilire una connessione sicura. Tuttavia, il browser non si fida di qualsiasi certificato, ma solo di quelli emessi da una lista di emittenti di certificati affidabili, conosciuti come root store. **Google** ha annunciato l'eliminazione di almeno un emittente di certificati da questo elenco.

Chi viene cacciato?

In un post pubblicato oggi sul *Google Security Blog*, l'azienda ha individuato l'autorità di certificazione (**CA**) **Entrust**. Non sembra che Entrust abbia commesso un singolo errore, ma piuttosto una serie di comportamenti che hanno portato a questa decisione. Le CA devono superare vari ostacoli per entrare nella lista dei buoni di Google e, secondo il post, Entrust ha *"disatteso"* le aspettative. Google non usa mezzi termini nel dichiarare che le azioni di Entrust hanno *"eroso la fiducia nella loro competenza, affidabilità e integrità come proprietario di una CA di fiducia pubblica"*.

L'esclusione di Entrust non avverrà immediatamente. Qualsiasi certificato Entrust emesso dopo il 31 ottobre 2024 non sarà più considerato attendibile da **Google Chrome**. Questo non significa che gli utenti di Chrome perderanno l'accesso a tutti i siti che utilizzano certificati Entrust, ma dovranno abilitare manualmente la fiducia in Entrust o superare una schermata di avviso quando visitano tali siti. Tali modifiche interesseranno tutti gli utenti di Chrome, tranne quelli su **iOS**.

Perché dovreste preoccuparvi dei certificati

Se avete navigato su internet, probabilmente avete visto qualche avviso di certificato nel vostro browser. Di solito, andare su uno di questi siti *"pericolosi"* designati dal browser non è un grosso problema, ma è importante sapere che questi siti probabilmente non utilizzano la crittografia per trasferire i dati tra il server e il browser. Ciò significa che qualcuno potrebbe intercettare i vostri dati, come nome utente e password. Non utilizzate informazioni personali su un sito non sicuro. Un certificato aggiornato è anche segno di un sito che prende sul serio la sua sicurezza.

Poiché i siti che utilizzano Entrust appariranno ora come inaffidabili, molti grandi nomi di internet si stanno probabilmente affrettando a cambiare il proprio fornitore di certificati. Vale la pena notare che Entrust è attualmente *nell'elenco delle CA affidabili* di **Firefox**, ma dato che Chrome controlla oltre il 65% del mercato dei browser, l'opinione di Firefox su Entrust non è in grado di spostare l'ago della bilancia.