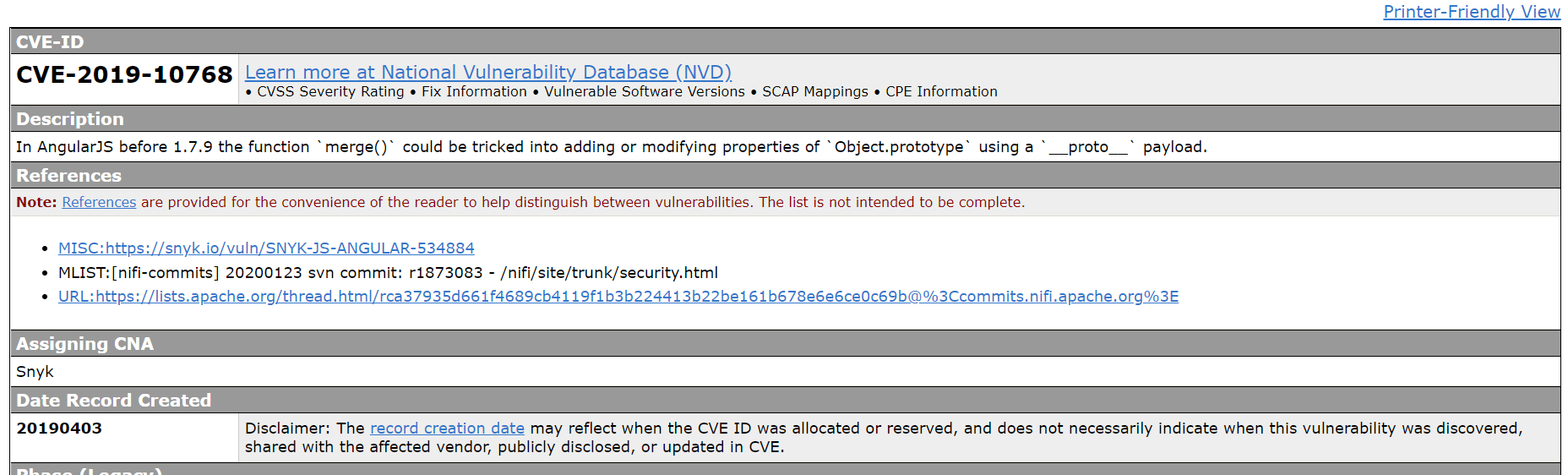
**CVE-2019-10768**

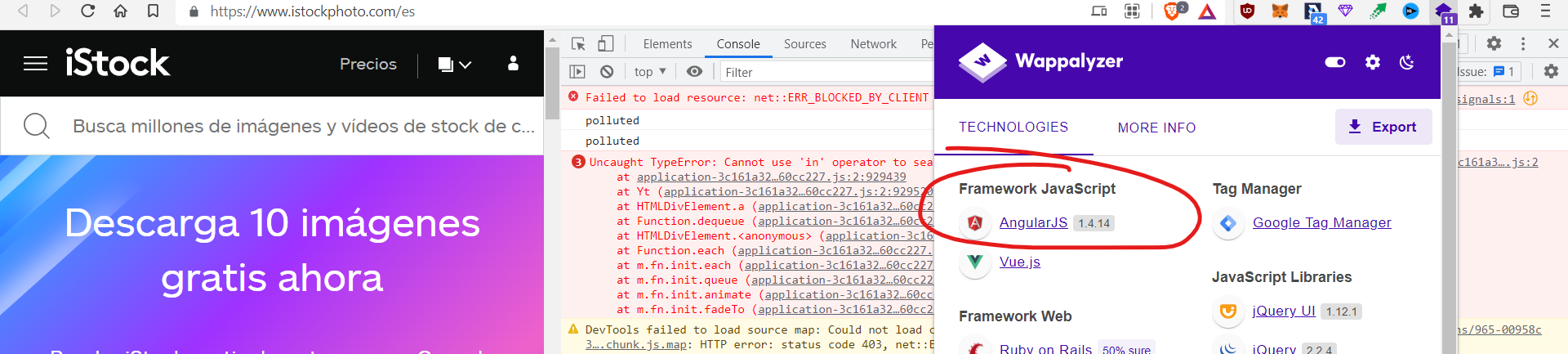
La información sobre la vulnerabilidad *CVE-2019-10768* se encuentra en la siguiente imagen:



Como se ve, es una vulnerabilidad que se puede explotar en páginas web que utilicen *AngularJS* en versiones anteriores a la 1.7.8.

Para realizar un escaneo de páginas web para ver si alguna tenía una versión anterior a la 1.7.8, he utilizado la extensión para *Chrome*, *Wappalyzer*. Buscando, he encontrado una (y bastante conocida), <https://www.istockphoto.com/>

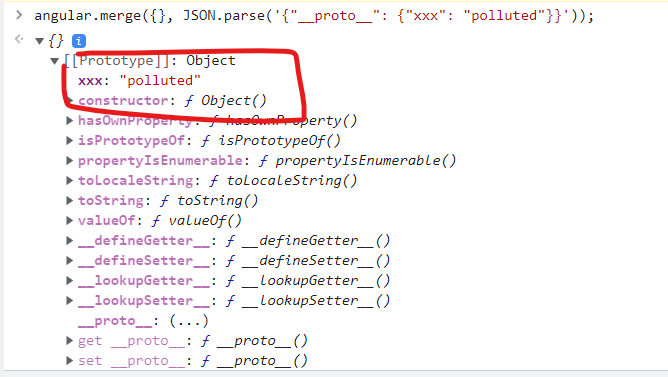
Utilizando la extensión, he verificado que utiliza una versión de AngularJS anterior a 1.7.8.



Una vez verificado, he probado la vulnerabilidad en la página web con la siguiente instrucción:

*angular.merge({}, JSON.parse('{"\_\_proto\_\_": {"xxx": "polluted"}}'));*

A lo que la página web ha devuelto:

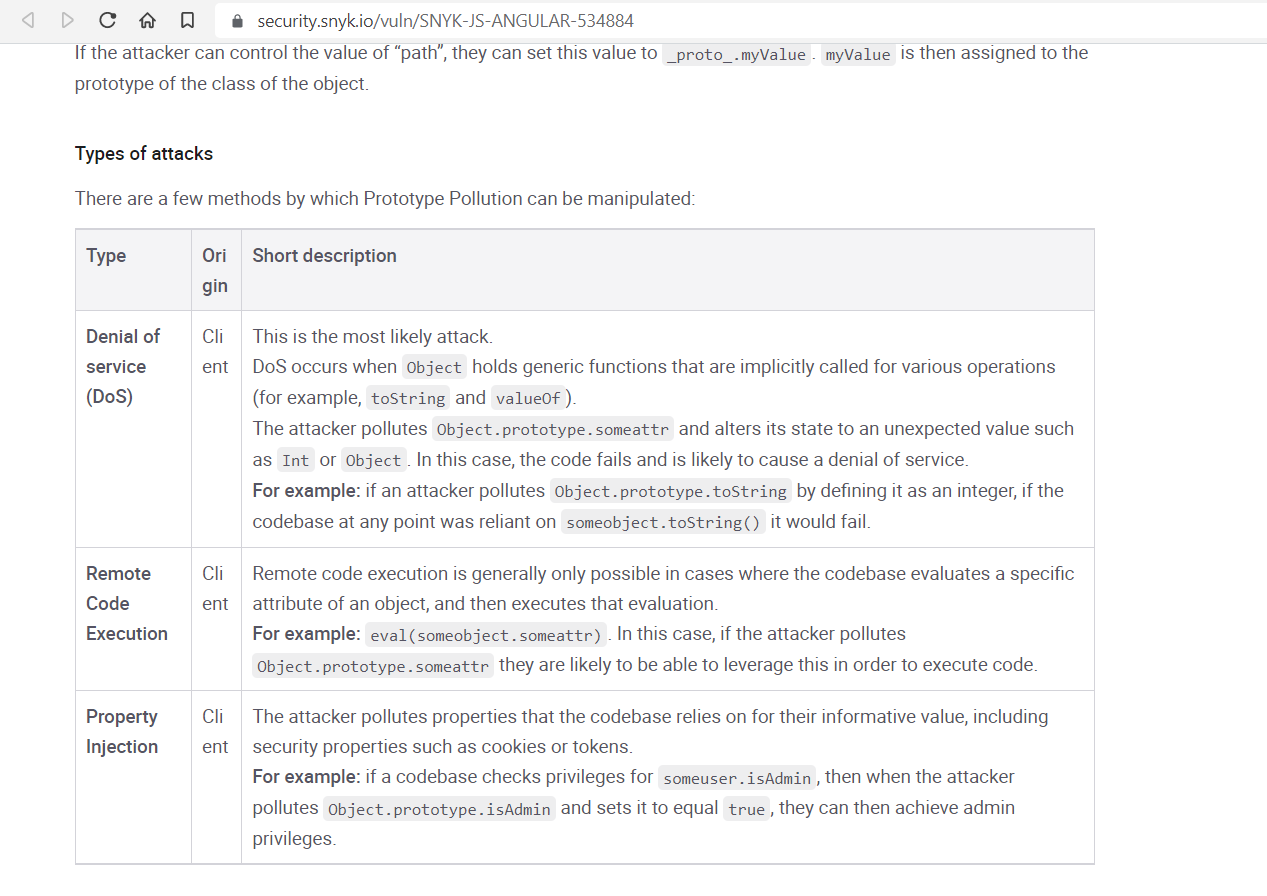


Para verificarlo de una manera más sencilla, he utilizado la siguiente instrucción que lo ha verificado:

*console.log(({}).xxx)*

Con esto, se puede confirmar que <https://www.istockphoto.com/> actualmente (día 08/03/2022) es vulnerable a la vulnerabilidad *CVE-2019-10768.*

Investigando sobre qué ataques se podrían intentar gracias a la vulnerabilidad, <https://security.snyk.io/vuln/SNYK-JS-ANGULAR-534884> nos da la siguiente información:



Para terminar, junto a este *PDF*, también se adjuntará un breve vídeo mostrando en directo la vulnerabilidad.

Bibliografía:

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-10768>

<https://security.snyk.io/vuln/SNYK-JS-ANGULAR-534884>

<https://www.youtube.com/watch?v=VVtNy7DbXAs>

Otros enlaces útiles:

<https://chrome.google.com/webstore/detail/wappalyzer-technology-pro/gppongmhjkpfnbhagpmjfkannfbllamg?hl=es>

<https://www.istockphoto.com/es>