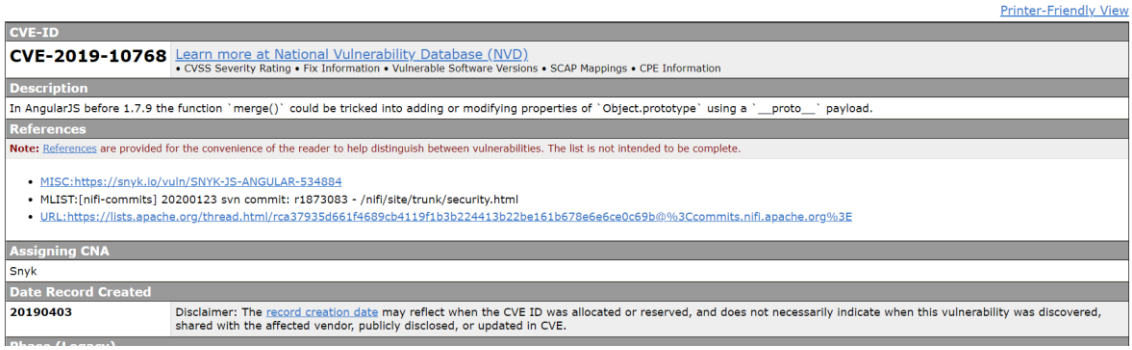
CVE-2019-10768

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



Printer-Friendly View

CVE-ID

CVE-2019-10768 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

In AngularJS before 1.7.9 the function `merge()` could be tricked into adding or modifying properties of `Object.prototype` using a `__proto__` payload.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://snyk.io/vuln/SNYK-JS-ANGULAR-534884
- MLIST:[nifi-commits] 20200123 svn commit: r1873083 - /nifi/site/trunk/security.html
- URL:https://lists.apache.org/thread.html/rca37935d661f4689cb4119f1b3b224413b22be161b678e6e6ce0c69b@%3Ccommits.nifi.apache.org%3E

Assigning CNA

Snyk

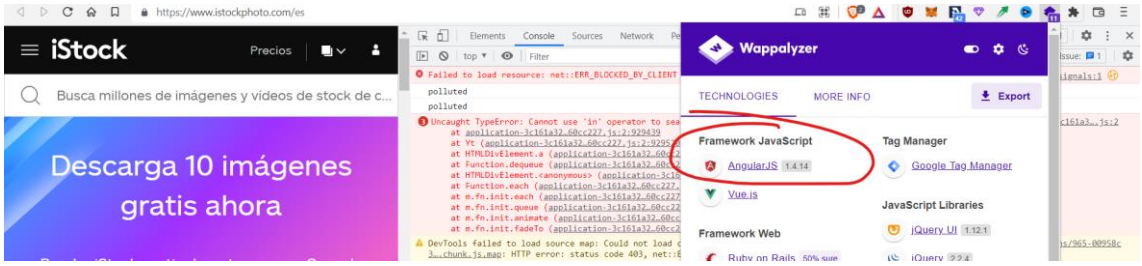
Date Record Created

20190403 Disclaimer: The record creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

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/

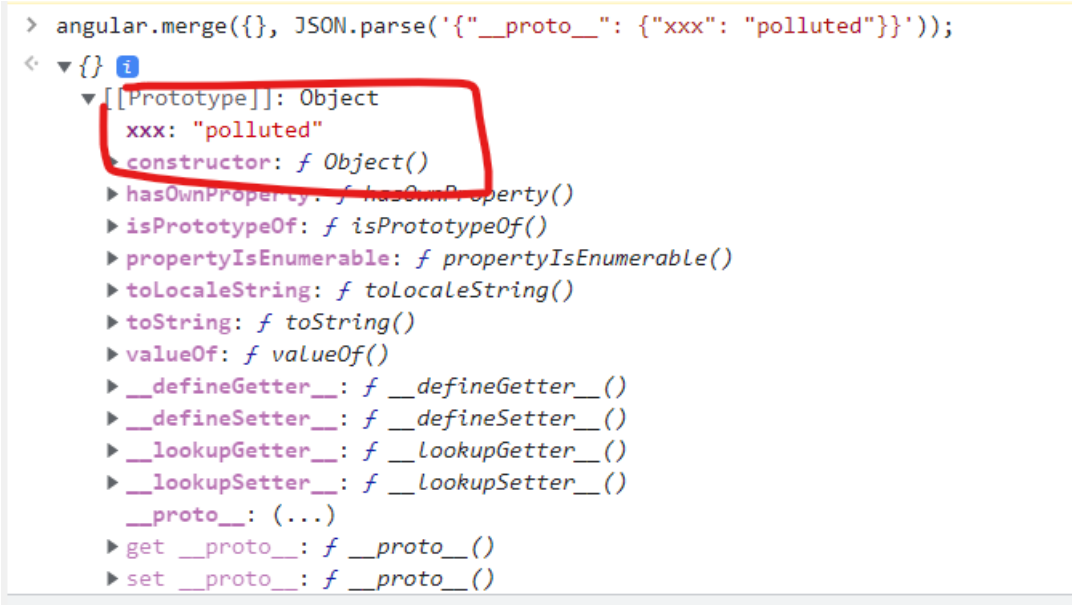
Utilizando la extensión, he verificado que utiliza una versión de AngularJS anterior a 1.7.8.



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:

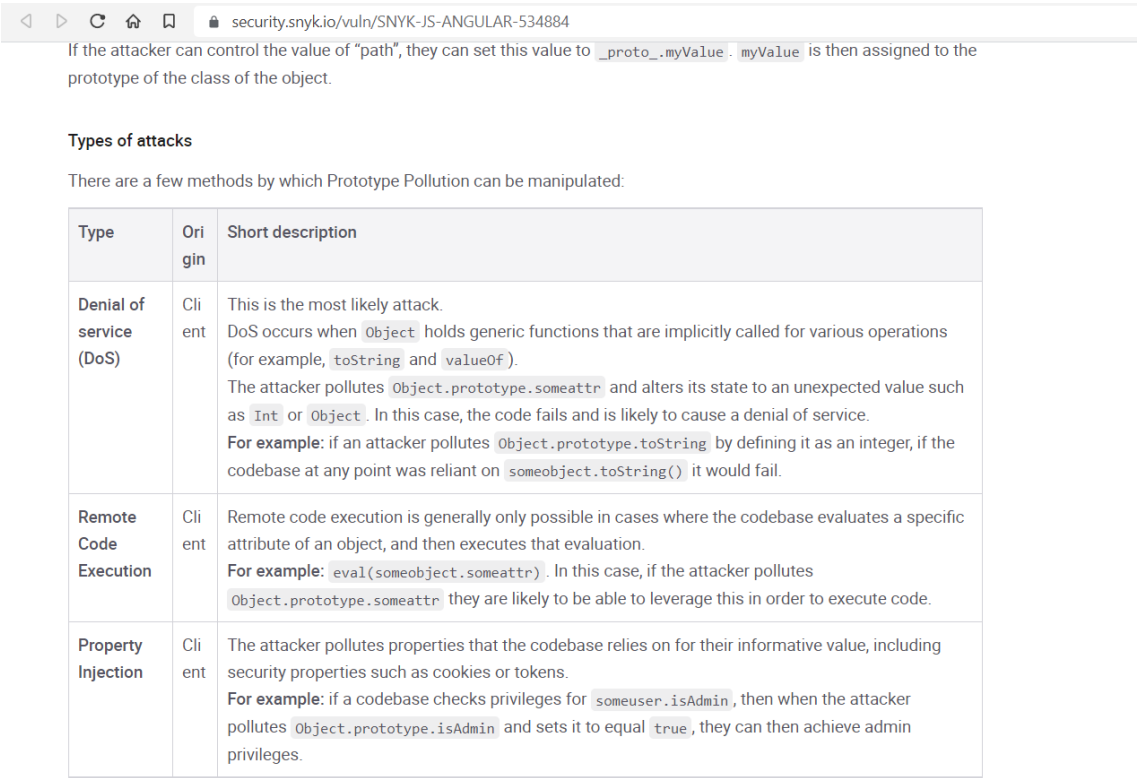


Para verificarlo de una manera más sencilla, he utilizado la siguiente instrucción que lo ha verificado:

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