jQuery is Outdated

Bu zafiyet jQuery kütüphanesinin güncel versiyonunun web uygulamasında kullanılmamasını ifade etmektedir. Bu yazı ise çoğu web geliştiricisinin jQuery kütüphanesinin en güncel versiyonunu kullandığını zannederken aslında nasıl eski versiyonunu kullandığını gösterecektir.

jQuery'nin resmi sitesinin yayınladığı jquery stabil versiyonları şu şekildedir:

jQuery 1.x
jQuery 2.x
JQuery 3.x

Bu kütüphaneler indirilip web uygulamasına eklenebileceği gibi CDN linkleri ile de web uygulamasına dahil edilebilir. Web geliştiricileri iş yükünü azalttığını düşündükleri

https://code.jquery.com/jquery-latest.min.js

CDN'inini kullanmaktalar. Bu CDN'in iş yükünü azalttığını düşünmektedirler, çünkü bu linkteki dosya ismi (jquery-latest.min.js) geliştiricilere dinamik olarak sürekli en güncel jQuery kütüphanesini çekiyoruz imajı doğurmaktadır. Fakat artık bu CDN güncellenmeyecekmiş ve ilelebet eski versiyonda bırakılacakmış (bkz: https://blog.jquery.com/2014/07/03/dont-use-jquery-latest-js/) Dolayısıyla çoğu web geliştiricisi jQuery dosya ismindeki latest kelimesine bakarak yanılgıya düşmekte ve son versiyonu kullanıyorum derken eski jQuery kütüphanesini kullanmakta. Bu sorunu çözmek için kesinlikle jquery-latest.min.js dosyası kullanılmamaldır. jQuery'nin resmi sitesinden en son jQuery kütüphanesine ait CDN linki alınmalıdır ve projede o link kullanılmalıdır. Her yeni jQuery güncellemesinde ise projedeki CDN linki elle güncellenmelidir.

Uygulama // Birebir gözlemlenmiştir.

xyz.org web uygulamasına yaptığım pentest'te Netsparker aracı hedef web uygulamasında aşağıdaki CDN'in kullanıldığını tespit etmiştir.

https://code.jquery.com/**jquery-latest.min.js**

Output:

v1.11.1 // Outdated

jQuery'nin resmi sitesi ise v1.x serisinin en son versiyonu olarak jQuery v1.12.4'ün var olduğunu söylemektedir. Dolayısıyla xyz web uygulaması geliştiricisi jquery-latest.min.js dosya ismine bakarak en son versiyonu kullandığını sanarken aslında eski bir jQuery kütüphanesini kullanmaktadır. Dolayısıyla web uygulamasındaki CDN linki son jQuery kütüphanesinin linki olarak değiştirilmelidir.

Şöyle ki web uygulamasında yer alan aşağıdaki kod

```
<script src="https://code.jquery.com/jquery-latest.min.js"></script>
```

aşağıdaki şekilde güncellenmelidir:

```
<script src="https://code.jquery.com/jquery-1.12.4.min.js "></script>
```

Her yeni çıkan jQuery güncellemesi sonrası ise CDN linki elle güncellenmelidir.

Kaynak

https://blog.jquery.com/2014/07/03/dont-use-jquery-latest-js/