There are no translations available.

Компанията за информационна и интернет сигурност Trend Micro пусна специален инструмент, чрез който мобилните и десктоп потребителите, които ползват Google Chrome, могат да проверят, дали даден сайт е уязвим на Heartbleed бъга.

Heartbleed Detector, както е и името на инструмента може вече да бъде свален от потребителите на Android от официалния магазин за мобилни приложения Goole Play
или от
Chrome Web Store
за потребителите на браузъра на Google.

С помощта на мобилното приложение, потребителите му ще могат да проверят, дали версията на OpenSSL в използваната от тях версия на Android е уязвима на бъга. Освен това потребителите ще могат да видят, дали някоя от библиотеките, които се ползват от инсталираните на устройствата им приложения не е уязвима на Heartbleed, а също така ще могат да разберат комуникират ли си някои от приложенията на устройствата им с уязвими сървъри.

Ако след сканирането за уязвими приложения бъде засечено такова, то на потребителят ще му се предложи деинсталиране на приложението, поясняват от компанията .

"Не препоръчваме на потребителите веднага да деинсталират засеченото приложение, но това е нещо, над което всеки трябва да се замисли, особено, ако се отнася за приложение, което обработва данни, които не трябва да стават достояние на външна страна, като например приложения за мобилно банкиране", пишат на сайта на компанията.

Ако пък не смятате да се възползвате от мобилното приложение и нямате инсталиран браузър Chrome, то тогава може да се възползвате от специален за целта сайт , на който може да разберете, дали дадена страница е уязвима или не.

Heartbleed е уязвимост, която бе открита в началото на този месец, притесненията около която продължават да нарастват с всеки изминал ден. Става дума за бъг в OpenSSL, открития стандарт за защита на комуникацията между сървър-клиент. Компрометирането на уязвимостта може да доведе до разкриване на съхраняваните данни на сървъра, защитени от протокола, като освен самите данни може да се случи и разкриване на тайните ключове, с които сървъра защитава данните.

Методи Дамянов, kaldata.com