# Stagefright za iPhone

Sjećate li se ozbiljnog propusta za Androidom pogonjene uređaje, nazvanog Stagefright [1]? Uistinu nezgodan propust kojim je napadač mogao, slanjem posebno formatirane MMS poruke, provaliti na mobilni uređaj.

Ako je itko od korisnika iOS uređaja do sad imao kompleks superiornosti nad korisnicima Androida ("nama se tako nešto nikad ne bi moglo dogoditi"), vrijeme je za otrežnjenje: propust CVE-2016-4631 [2] u Image I/O API dozvoljava napadaču da na vrlo sličan način, slanjem posebno formatirane TIFF [3] datoteke izvrši maliciozni kod korištenjem heap overflow [4] napada.

Zanimljivo je da je riječ o propustu koji, slijedom slučajnih događaja, neodoljivo podsjeća na **Stagefright**: u oba slučaja otkriveni su nedostaci u biblioteci koja se bavi nekim multimedijalnim sadržajem i koja je dio operacijskog sustava (što znači da postoji mnogo potencijalnih mjesta upada, faktički svaka aplikacija koja koristi ranjivu biblioteku je izložena napadu). Način provale je vrlo sličan u oba slučaja, a i najkritičniji dio propusta: vektor prijenosa malicioznog koda – u oba slučaja je gotovo identičan.

Prema navodima [5] Cisco TALOS grupe koja je otkrila ove nedostatke, formati grafičkih datoteka osjetljivi na napade su TIFF, BMP, EXR (OpenEXR) i DAE (Digital Asset Exchange/COLLADA).

Platforme izležene ovoj ranjivosti su OS X Mavericks, OS X Yosemite, OSX El Capitan, iOS 9.3.2, watchOS 2.2.1 i tvOS 9.2.1.

Srećom, Apple je u mogućnosti izdati centralizirane zakrpe za sve svoje operacijske sustave, što rješavanje ovog problema čini značajno lakšim u odnosu na **Stagefright** i fragmentiranu Android platformu. Time je i rješenje ovog problema posve trivijalno, jednom riječju: "update".

pon, 2016-08-01 11:31 - Radoslav Dejanović**Vijesti:** Sigurnost [6]
**Vote:** 0

No votes yet

**Source URL:** https://sysportal.carnet.hr/node/1668

**Links**
[1] https://sysportal.carnet.hr/node/1657
[2] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4631
[3] https://en.wikipedia.org/wiki/Tagged_Image_File_Format
[4] https://en.wikipedia.org/wiki/Heap_overflow

[5] http://blog.talosintel.com/2016/07/apple-image-rce.html
[6] https://sysportal.carnet.hr/taxonomy/term/13