CONFIG_KEYS sigurnosni propust

Nedavno je otkriven sigurnosni propust u Linuxovu kernelu koji pogađa sve jezgre od verzije 3.8 na dalje, a koji napadaču omogućuje dobivanje administratorskih ovlasti.

Ovaj sigurnosni propust vjerojatno ne bi izazvao toliko pažnje da se konačno i na primjeru Linuxove jezgre nije pokazala opasnost monokulture: svi sustavi koji koriste Linux kernel osjetljivi su na taj napad. Prema informacijama do kojih su došli autori otkrića to uključuje i otprilike dvije trećine svih Android uređaja na tržištu, što su novinari jedva dočekali - sigurnosni problemi Android uređaja ipak su mnogo zanimljiviji od sigurnosnih problema Linux poslužitelja.

Tako se čini manje dramatičnom informacija da je propust tu već gotovo tri godine, koliko činjenica da je ranjiv ogroman broj korisničkih i IoT uređaja. Novinari su u određenom smislu u pravu: sistemci znaju da će, ako već nisu, vrlo brzo dobiti novu verziju kernela s ispravljenim propustom (ili ga kompajlirati sami, oni parano^H^H^H^H^Hoduzetniji). S druge strane proizvođači mobilnih uređaja nisu tako ažurni u izdavanju sigurnosnih zakrpa, pa možemo očekivati kako će ovaj sigurnosni propust u Android ekosustavu nestati tek prirodnim "odumiranjem" starih uređaja i njihovom zamjenom novim uređajima.

U kakvoj su opasnosti korisnici Android uređaja koji neće dočekati sigurnosnu zakrpu?

Nećemo se baviti Linux serverima jer će oni vjerojatno već biti pokrpani u trenutku kad budete čitali ovaj tekst, ali svaki pošten sistemac ima barem jedan Android "gadget" kojeg ne može zakrpati. Napad treba izvesti na lokalnom stroju, dakle nije riječ o nečem što će vas samo tako napasti s Interneta. Najčešći vektor zaraze Android uređaja instalacija je zaraženih programa s neslužbenih repozitorija (na kojima se lako nađu besplatne, tek malo "posoljene", verzije komercijalnih aplikacija iz Google Play trgovine).

Ako je korisnik instalirao *malware* koji zna iskoristiti ovaj propust, to i dalje neće biti lak posao: napadač mora izvesti četiri milijarde inkrementalnih operacija nad varijablom "usage", nakon čega ona biva postavljena na nulu, što otvara prostor za use-after-free [1] napad.

Malo jačem stolnom računalu treba oko pola sata za izvođenje napada, dok Android uređajima i njihovim respektabilnim, ali ipak slabijim procesorima za to treba mnogo, mnogo više vremena.

Naravno, napadaču koji je već na uređaj postavio aplikaciju koja izvršava napad vrijeme nije od presudne važnosti, pa se napad može odvijati satima, sve dok se aplikacija ne istrgne iz *sandboxa* ili iscrpi baterija. Skeptici bi ovom poprilično sporom napadu dodali i činjenicu da izvorni podatak o dvije trećine svih Android uređaja možda i nije baš posve točan, jer kernel koji se kompajlira za Android obično nema uključenu CONFIG_KEYS varijablu (što, naravno, ovisi od slučaja do slučaja), te činjenica da uređaji koji koriste Android 5.0 ili noviji nisu osjetljivi na napad, kao i oni koji koriste verzije Androida izašle prije KitKata.

Trebate li brinuti? Pa... ako imate običaj instalirati egzotične APK-ove, vjerojatno da: jednom instaliran, malware će polako ali sigurno izaći iz svog pješčanika i nakon toga sva su mu vrata otvorena – ali ponovo, najviše zato što proizvođači uređaja ne mare za sigurnost robe koju su već prodali.

Na Linux računalim panici nema mjesta, jer za ovaj propust nije primjećen exploit "u divljini". Ali kako smo već spomenuli, ovo je lijep primjer širine opasnosti koju donosi monokultura.

pet, 2016-01-22 14:49 - Radoslav Dejanović**Vijesti:** Sigurnost [2]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

Source URL: https://sysportal.carnet.hr/node/1596

Links
[1] https://cwe.mitre.org/data/definitions/416.html
[2] https://sysportal.carnet.hr/taxonomy/term/13