Nesigurni sigurnosni uređaji

Većina specijaliziranih uređaja čija je namjena poboljšanje sigurnosti, poput e-mail gatewaya, vatrozida, IPS-ova i slično, nije prošla provjere ranjivosti. Najčešći uzroci ranjivosti su pogreške u web sučelju i loše održavan i konfiguriran operacijski sustav.

Rezultate svog istraživanja iznio je penetracijski tester Ben Williams, zaposlen u NCC Groupi, na svom predavanju na Europskoj Black Hat konferenciji 2013. Naslov njegova izlaganja je "Ironic Exploitation of Security Products".

Wiliams je testirao proizvode poznatih tvtrki, među kojima su Symantec, Sophos, Trend Micro, Cisco, Baracuda, McAfee i Citrix. Dio uređaja je provjeren u sklopu penetracijskih testova, dio u sklopu testova uređaja koje su naručili kupci, a dio u slobodno vrijeme. Rezultati su više nego zanimljivi: na više od 80 % uređaja pronađene su ozbiljne ranjivosti koje nije bilo teško otkriti. Većina je pronađena u web sučeljima koja nemaju zaštitu od napada pogađanjem zaporki, a ranjiva su i na *cross-site scripting* i *session hijacking* napade. Mnogi od uređaja pokazuju informacije o verziji i modelu proizvoda neautenticiranim korisnicima, što napadačima olakšava posao. Među otkrivenim ranjivostima su i *cross-site request forgery*, navođenje administratora da posjeti maliciozne web stranice, da bi se nakon toga dobilo pristup administrativnim funkcijama. Mnogi uređaji ranjivi su na *command injection* i eskalaciju privilegija. Nešto rjeđe pronađene su ranjivosti koje omogućavaju zaobilaženje autentikacije, napade uskraćivanja usluge (DoS), a pronađen je loše konfiguriran SSH servis.

Proizvođači oglašavaju da njihovi proizvodi koriste sigurnu verziju Linuxa, no istraživanje je pokazalo da to naprosto nije istina. Obično je to neka verzija Linuxa sa zastarjelim kernelom, instaliranim nepotrebnim paketima i lošom konfiguracijom. Ne koriste se uobičajene metode zaštite, SELinux i AppArmour.

Preko 50% uređaja dozvoljavalo je administrativni pristup web sučelju iz vanjske mreže, izlažući se tako napadima. Williams savjetuje korisnicima da web pristup omoguće samo iz lokalne mreže, a administratorima da ne koriste preglednik s kojim inače surfaju, nego na primjer Firefox s uključenom ekstenzijom NoScript.

Williams je o rezulatima istraživanja obavijestio proizvođače, koji su reagirali na različite načine. Neki su informacije podijelili s korisnicima i potrudili se zaštiti svoje uređaje. No ironično je da su tolike ranjivosti pronađene na proizvodima tvrtki specijaliziranih za informacijsku sigurnost, što bi upućivalo na to da je kod ostalih proizvođača situacija vjerojatno još lošija.

Na prezentaciji je Williams demonstrirao napade na nekolicinu uređaja koji omogućuju dobijanje pune kontrole nad sigurnosnim uređajima. Rezltati istraživanja objavljeni su na stranicama NCC Grupe [1].

pon, 2013-04-15 11:19 - Aco Dmitrović**Vijesti:** Sigurnosni propusti [2]
Kategorije: Sigurnost [3]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1248

Links
[1] http://www.nccgroup.com/media/230493/hacking_appliances_whitepaper_ben_williams_1.1.pdf
[2] https://sysportal.carnet.hr/taxonomy/term/14
[3] https://sysportal.carnet.hr/taxonomy/term/30