PGP/GPG i S/MIME eksfiltracija podataka zbog loše napisanih klijentskih aplikacija

Grupa istraživača najavila je za utorak objavu jednog ili više značajnih propusta u PGP/GPG i S/MIME enkripciji, a EFF je preporučio izbjegavanje korištenja PGP-a u e-mail komunikaciji. Štura najava(https://www.eff.org/deeplinks/2018/05/attention-pgp-users-new-vulnerabilities-require-you-take-action-now [1]) djeluje poprilično uznemirujuće: sigurnosni propust omogućuje čitanje novih i starih poruka (što nije iznenađujuće), ali EFF savjetuje isključivanje ili brisanje svih dodataka za programe za elektroničku poštu koji omogućuju automatizirano dekodiranje zaštićenih poruka (Enigmail za Thunderbird, GPGTools za Mac, GPG4Win za Outlook), uz dodatno napisane upute kako isključiti ili obrisati te dodatke.

Ovo je uznemirujuća vijest, jer iako ne možemo trenutno sa sigurnošću znati ništa (pa ni kakvo se to zlo krije u automatiziranom otključavanju zaštićene poruke), uputa za ovako drastičan korak ne sluti na dobro.
S druge strane, pojavili su se komentari da je problem jednostavno rješiv isključivanjem HTML podrške u programu za čitanje email poruka, jer se eksfiltracija dekodiranih podataka obavlja pozivom prema udaljenom poslužitelju sa tijelom poruke unutar zahtjeva: drugim riječima, zbog loše izolacije sustava - a PGP propust zapravo ne postoji, jer je krivac loše napisan program za čitanje elektroničke pošte.

O čemu se točno radi saznat ćemo uskoro, a na vama je da odlučite želite li poslušati savjet EFF. U svakom slučaju, EFF savjetuje barem privremeni prelazak na druge oblike zaštićene komunikacije dok se uočeni problemi ne riješe i eksfiltracija ne onemogući.

Neslužbeni whitepaper (draft 0.9.0 u trenutku pisanja ovog teksta) moguće je pronaći ovdje: https://efail.de/efail-attack-paper.pdf [2]

sri, 2018-05-16 12:39 - Radoslav Dejanović**Vijesti:** Sigurnosni propusti [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: PGP [4]
GPG [5]
S/MIME [6]

Source URL: https://sysportal.carnet.hr/node/1809

Links
[1] https://www.eff.org/deeplinks/2018/05/attention-pgp-users-new-vulnerabilities-require-you-take-

action-now
[2] https://efail.de/efail-attack-paper.pdf
[3] https://sysportal.carnet.hr/taxonomy/term/14
[4] https://sysportal.carnet.hr/taxonomy/term/239
[5] https://sysportal.carnet.hr/taxonomy/term/240
[6] https://sysportal.carnet.hr/taxonomy/term/241