Windows 10 ranjivi radi pogrešne provjere certifikata


NSA je otkrila propust u provjeri certifikata koji Windowse 10 čini ranjivima tako što omogućava instalaciju zlonamjernog softvera. Propust je prijavljen pod oznakom CVE-2020-0601, a Microsoft je po brzom postupku izdao zakrpu u utorak 14.1.2020.

Analitičari hvale pristup NSA koja je ranjivost najprije prijavila Microsoftu, kako bi se propust što prije otklonio. Zar su trebali postupiti drugačije? :)

U opisu ranjivosti stoji: Otkrivena je ranjivost u načinu na koji Windows CryptoAPI (Crypt32.dll) provjerava Elliptic Curve Cryptography (ECC) certifikate. Napadač bi mogao iskoristiti ranjivost izradom lažnog certifikata kojim bi potpisao maliciozni program, čime bi se on predstavljao da dolazi od provjerenog, legitimnog izvora. Ranjivost je nazvana 'Windows CryptoAPI Spoofing Vulnerability'.

Savjete Microsofta i linkove na zakrpe potražite ovdje: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601 [1]

Kao dodatna prijetnja navodi se da bi exploit dozvolio man-in-the-middle napad i dekriptiranje povjerljivih informacija tako što bi se veze prema napadačkim računalima predstavljale kao da su sigurne, a podaci koji dolaze s njih kao provjereni.

Instalacijom zakrpa omogućit će se potpuna i ispravna provjera certifikata, pa bi rizici bili uklonjeni. Narednih tjedana očekuju se napadi na računala koja nemaju instaliranu zakrpu, zato ne bi trebalo odgađati njihovu instalaciju.

Čini se da je u zadnje vrijeme bilo problema s Microsoftovim zakrpama, neki su korisnici prijavljivali da im se nakon instalacije zakrpa pojavljivao zloglasni *Blue Screen of Death* (BSOD). Zato bi bilo dobro isprobati nove zakrpe na testnom računalu u labosu. :) Nedostatak pravog laboratorija sistemac može kompenzirati instalacijom virtualke, izradom snapshota, sa ispravnim stanjem, pa zatim instalacijom zakrpa. Ukoliko se nakon instaliranja zakrpe pojave problemi, može se problem prijaviti i odgoditi instalaciju zakrpa.

Mada, iskusan sistemac će vam reći da zakrpe ponekad prođu bez greške na desetak računala, da bi se na jedanaestom pojavio BSOD. :)

Šalu na stranu, isprobajte zakrpu, instalirajte je na sva Windows 10 računala, radi se o propustu koi bi mogao imati dalekosežne (loše) posljedice.

čet, 2020-01-16 16:09 - Aco Dmitrović**Vijesti:** Windows [2]
Kategorije: Sigurnost [3]
Vote: 5

Vaša ocjena: Nema Average: 5 (1 vote)

story_tag: sigurnost [4]
windows 10 [5]

Windows CryptoAPI Spoofing [6]

Source URL: https://sysportal.carnet.hr/node/1862

Links
[1] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
[2] https://sysportal.carnet.hr/taxonomy/term/12
[3] https://sysportal.carnet.hr/taxonomy/term/30
[4] https://sysportal.carnet.hr/taxonomy/term/82
[5] https://sysportal.carnet.hr/taxonomy/term/175
[6] https://sysportal.carnet.hr/taxonomy/term/349