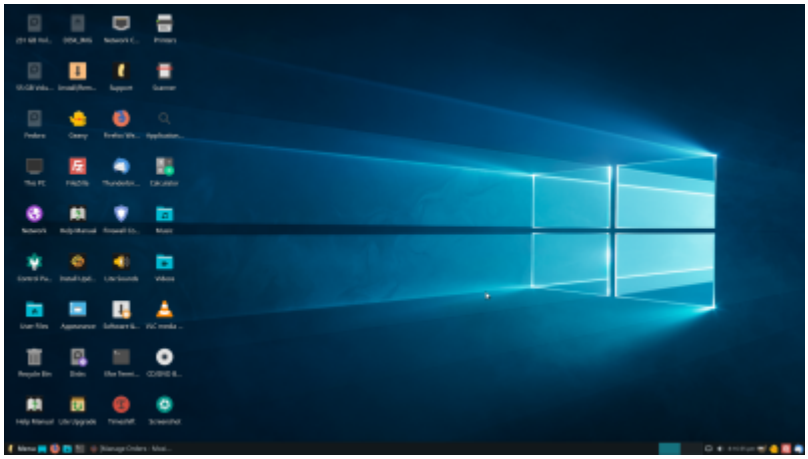
Scris de newsreporter pe 01 august 2020, 10:23

O noua vulnerabilitate pentru Windows si Linux

Lasand la o parte numele cu rezonanta ciudata, BootHole este un bug localizat tocmai in codul de initializare a PC-urilor Windows si Linux, care poate fi exploatat pentru a incarca in mod nedetectabil aplicatii malware, scrie descopera.ro.



Windows-12-Lite-Desktop.png

Prezent pe orice computer care functioneaza prin incarcarea unui sistem de operare, sistemul bootloader este primul element software care se initializeaza la pornirea unui PC, rolul sau fiind de a permite selectarea si apoi initializarea sistemului de operare principal, fie ca acesta este Windows sau Linux. Lesne de inteles, oricine reuseste sa compromita securitatea componentei bootloader poate obtine acces nelimitat asupra computerului, inserand elemente malware in mod aproape complet nedetectabil. si, in timp ce PC-urile Linux sunt direct expuse vulnerabilitatii BootHole,aproape toate computerele Windows din ultimul deceniu sunt, de asemenea, vulnerabile.Concret, in centrul acestei vulnerabilitati se afla componenta UEFI Secure Boot, responsabila tocmai cu securizarea procesului de pornirea a PC-ului prin autentificarea software-ului ce urmeaza a fi incarcat. Prezent inclusiv la dispozitive smartphone si tablete, sistemul UEFI Secure Boot este ceea ce modderii trebuie mai intai sa deblocheze pentru accesarea sistemului bootloader, facilitand incarcarea de versiuni firmware neoficiale.

BootHoole pacaleste mecanismul de validare prin semnatura digitala a versiunilor de firmware

Problema apare atunci cand bootloader-ul in sine contine o vulnerabilitatea care poate fi exploatata pentru a obtine acces privilegiat la un sistem altfel sigur, cum este meniul GRUB2 folosit de aproape toate distributiile Linux

. Un bootloader ruleaza cu mai multe privilegii de acces decat sistemul de operare, iar singura sa verificare se face la pornirea PC-ului, prin cod semnat sau certificat. Daca un hacker este capabil sa suprascrie un bootloader cu o versiune recunoscuta, dar vulnerabila, procesul de incarcare Secure Boot nu poate detecta abuzul comis.

Citeste continuarea pe Go4it!

ADRESA: http://crct.ro/nwsl