Apple IOS

Zbulohet nje vulnerabilitet “zero day” ne aplikacionin e emailit te IOS, prezent qe prej 8 vjetesh.

Vulnerabilitetet që fillojnë me versionin iOS 6, të cilat shkaktohen përmes aplikacionit të emailit në iOS, janë zbuluar se nëse shfrytëzohen, lejojnë ekzekutimin e kodit në distancë.

Problemet u zbuluan nga firma e sigurisë ZecOps, e cila ka vërejtur këtë dobësinë në versionin iOS 11.2.2 qysh në nëntor 2018 dhe potencialisht edhe më herët. Apple u informua në shkurt 2019 dhe kompania lëshoi një "patch" beta në prill duke korrigjuar çështjen.Ky vulnerabilitet prek vetëm aplikacioni e postës elektronike të iOS , dhe jo shumëllojshmërite e palëve të treta si Gmail ose Outlook.

“Dobësia lejon të ekzekutohet një kod ne distance në kontekstin e MobileMail (iOS 12) ose të dërguar me postë (iOS 13). Shfrytëzimi i suksesshëm i kësaj dobësie do të lejojë që sulmuesi të lexoje, modifikojë dhe fshijë email. Vulnerabilitete shtesë të kernelit do ti sigurojnë akses të plotë të pajisjes sulmuesit" raportohet nga ZecOps

Ajo që e bën këtë problem jashtëzakonisht të rrezikshëm është se në disa raste mund të lancohet vetëm duke hapur aplikacionin e postës elektronike.

Pronarët e pajisjeve mund ta kenë të vështirë ta kuptojene nëse janë prekur nga ky sulm. Shenjat e jashtme përfshijnë një ngadalësim të përgjithshëm të sistemit dhe në disa raste prishjen e aplikacionit të postës.

Ndërsa kjo dobësi është rregulluar në versionet Beta të zhvilluesve të IOS, është thelbësore që të nxirret nje version perfundimtar i "patch"-imit sa me shpejtë për përdoruesit për të siguruar pajisjet e tyre nga ky vulnerabilitet.Në varësi të rrezikut dhe konfidencialitetit të emailit të një punonjësi, një organizatë do të duhet të përcaktojë nëse ata do të ndalojnë përdorimin e aplikacionit të prekshëm derisa të lëshohet "patch".

Dobësitë janë shfrytëzuar nga shtete dhe organizatat profesionale të hakerave që sjellin një nivel shtesë të rrezikut për situatën.Ju duhet të supozoni se çdo sulmues me aftësi të mjaftueshme ose mbështetje financiare mund ti shfrytëzoje këto vulnerabilitete dhe të marri kontrollin e kompjuterave ose pajisjeve që drejtojnë ndonjë sistem operativ ose aplikim. Këto shfrytëzime janë krijuar posaçërisht për të mos u zbuluar nga antivirus, firewall ose kontrolle të tjera të sigurisë. E vetmja mënyrë për të mbrojtur kundër sulmuesve të tilla është të keni një kulturë të sigurisë me aftësi të thelluara të mbrojtjes, duke përfshirë monitorimin e ngushtë të regjistrave të sigurisë dhe trafikut anomal të rrjetit.