AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi të shfrytëzuara në mënyrë aktive në produktet e Apple

Data 25/03/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Dobësi të shumta në produktet e Apple po shfrytëzohen në mënyrë aktive për të fituar akses të paautorizuar, për të kompromentuar të dhëna sensitive dhe për të prishur sistemet e prekura.

Informacione Teknike

Në produktet Apple, duke përfshirë iOS, macOS dhe Safari, janë identifikuar shumë dobësi me ashpërsi të lartë. Këto dobësi shfrytëzohen në mënyrë aktive përmes përmbajtjes së krijuar në mënyrë keqdashëse në internet, zakonisht të shoqëruara me sulme të sofistikuara "të rrezikshme".

Këto dobësi janë pjesë e paketës së shfrytëzimit DarkSword, e cila është përdorur nga aktorë të shumtë kërcënimesh për të vendosur familje të avancuara të malware-it të afta për vjedhje të gjerë të të dhënave, vazhdimësi dhe ekzekutim të kodit në distancë.

Detajet e dobësive
Dobësi me ashpërsi të lartë
CVE-2025-31277
• Një dobësi e korruptimit të kujtesës në WebKit që mund të shkaktohet gjatë përpunimit të përmbajtjes së krijuar në mënyrë keqdashëse në internet. Shfrytëzimi i suksesshëm mund t'u lejojë sulmuesve të ekzekutojnë kod arbitrar brenda kontekstit të shfletuesit.

CVE-2025-43510
• Një dobësi e korruptimit të kujtesës në bërthamë që mund të lejojë një aplikacion dashakeq të manipulojë kujtesën e përbashkët midis proceseve, duke çuar potencialisht në përshkallëzim të privilegjeve ose kompromentim të sistemit.

CVE-2025-43520
• Një dobësi e korruptimit të memories kernel që mund të rezultojë në ndërprerje të papritur të sistemit ose të lejojë shkrimin në memorien, duke i mundësuar sulmuesve të fitojnë privilegje të larta ose të ekzekutojnë kod arbitrar.

Produktet e prekura
• Apple watchOS, iOS, iPadOS, macOS, visionOS, tvOS dhe iPadO

Rekomandime

AKSK rekomandon:

• Zbatoni përditësimet menjëherë: Sigurohuni që të gjitha pajisjet Apple të jenë të përditësuara në versionet më të fundit të disponueshme.

• Aktivizoni përditësimet automatike: Për të zvogëluar ekspozimin ndaj dobësive të ardhshme.
• Tregoni kujdes me përmbajtjen e uebit: Shmangni klikimin në lidhje të dyshimta ose vizitën në faqet e internetit të pabesueshme.
• Monitoroni sistemet: Shikoni për tregues të kompromentimit, veçanërisht aksesin e pazakontë të të dhënave ose paqëndrueshmërinë e sistemit.
• Vendosni kontrolle sigurie: Zbatoni monitorimin e rrjetit, mbrojtjen e pikave fundore dhe zgjidhjet e zbulimit të kërcënimeve.