AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Përditësime Sigurie – Apple

Data: 12/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Apple ka publikuar përditësime kritike sigurie në të gjithë ekosistemin e produkteve të saj, duke adresuar dobësi me rrezikshmëri të lartë që prekin:

- iOS
- iPadOS
- macOS
- tvOS
- watchOS
- visionOS
- Safari

Përditësimet korrigjojnë një numër të madh dobësish, përfshirë:

- një **zero-day aktivisht të shfrytëzuar**
- dobësi për dalje nga sandbox
- probleme të rritjes së privilegjeve në nivel kernel
- dobësi të korrupsionit të memories

Informacione Teknike

ZERO-DAY i Shfrytëzuar Aktivisht

CVE-2026-20700

- **Komponenti:** dyld
- **Ndikimi:** Sulmuesi mund të ekzekutojë kod arbitrar nëse ka aftësi për të shkruar në memorie
- **Rrezikshmëria:** Kritike
- **Statusi:** Apple ka raportime se është përdorur në sulme shumë të sofistikuara ndaj individëve të targetuar në versione të iOS para iOS 26
- **Shkaku:** Problem korrupsioni memorieje, i adresuar me përmirësim të menaxhimit të gjendjes
- **CVE të lidhura:** CVE-2025-14174, CVE-2025-43529

Dobësi të Tjera Kryesore

Rritje Privilegjesh

- CVE-2026-20617 – CoreServices (race condition)
- CVE-2026-20615 – CoreServices (trajtim path-i)

- CVE-2026-20626 – Kernel (app keqdashës)

Dalje nga Sandbox

- CVE-2026-20628 – Sandbox (leje të pasakta)
- CVE-2026-20667 – libxpc (gabim logjik)
- CVE-2026-20677 – Messages (race condition në symbolic links)

Sulme Rrjeti

- CVE-2026-20671 – Interceptim trafiku rrjeti
- CVE-2026-20660 – Shkrim skedari nga përdorues remote
- CVE-2026-20650 – DoS përmes paketave Bluetooth

Dobësi në WebKit / Safari

Dobësi të shumta në WebKit mund të shkaktojnë:

- rrëzim procesi nga përmbajtje web keqdashëse
- denial-of-service në distancë
- gjurmim përdoruesi përmes extensions Safari

Zbulim Informacioni dhe Privatësia

Dobësi që mund të lejojnë:

- shikim të të dhënave sensitive përmes aksesit fizik
- zbulim të memories përmes imazheve të manipuluara
- akses në foto apo informacion përdoruesi nga lock screen
- zbulim informacioni përmes log-eve ose aplikacioneve

Memory Corruption / Stabilitet Sistemi

Dobësi që mund të shkaktojnë:

- terminim sistemi ose kernel corruption
- crash aplikacionesh përmes file-eve ose mediave të manipuluara

Dobësi të tjera

Përfshijnë:

- akses të paautorizuar në histori Safari
- identifikim aplikacionesh të instaluara
- rrjedhje informacioni në Call History dhe Mail previews
- dobësi DoS nga komponentë open-source (p.sh. libexpat)
- crash përmes pajisjeve HID/Multi-Touch të manipuluara

Versionet e Përditësuara të Softuerit

- **iOS / iPadOS 26.3** – iPhone 11 dhe më të rinj
- **iOS / iPadOS 18.7.5** – pajisje më të vjetra (XS, XR, etj.)
- **macOS Tahoe 26.3**
- **macOS Sequoia 15.7.4**
- **macOS Sonoma 14.8.4**
- **tvOS 26.3**
- **watchOS 26.3**
- **visionOS 26.3**
- **Safari 26.3**

Rekomandime

Rekomandohet:

- Instaloni menjëherë versionet më të fundit të publikuara nga Apple.
- Monitoroni për çdo aktivitet të dyshimtë që mund të lidhet me shfrytëzimin e këtyre dobësive.

Referenca

https://support.apple.com/en-us/100100