AUTORITETI KOMBËTAR
PËR SIGURINË KIBERNETIKE

Dobësi të Shumta Kritike në SandboxJS

Data: 10/02/2026
Version: 1.0

Përmbajtja

Përmbledhje Ekzekutive

Janë identifikuar **katër dobësi kritike** në **SandboxJS**, një bibliotekë JavaScript e përdorur gjerësisht për sandboxing, e projektuar për të izoluar dhe siguruar ekzekutimin e kodit të pabesuar.
Të katër dobësitë janë vlerësuar me **rezultatin maksimal CVSS 10.0**, duke treguar **rrezikshmëri kritike**. Këto defekte u mundësojnë sulmuesve të **anashkalojnë plotësisht mekanizmat e sandbox-it** dhe të **ekzekutojnë kod arbitrar në sistemin host**, duke kompromentuar në mënyrë themelore garancitë e sigurisë që ofron biblioteka.

Informacione Teknike

Detaje të Dobësisë

1. CVE-2026-25520: Shfrytëzim i Vlerës së Kthimit të Funksioneve

- **CVSS Score:** 10.0 (Kritike)
- **Vektori i sulmit:** Shfrytëzon trajtimin e pasaktë të vlerave të kthimit të funksioneve
- **Mekanizmi i dobësisë:**
  - Vlerat e kthimit të funksioneve nuk mbështillen siç duhet nga sandbox-i
  - Sulmuesit mund të përdorin `Object.values` ose `Object.entries` për të marrë array që përmbajnë `Function constructor` të host-it
  - Jep akses të drejtpërdrejtë në ambientin e ekzekutimit të host-it
- **Ndikimi:** Dalje e plotë nga sandbox-i me aftësi për ekzekutim arbitrar kodi

2. CVE-2026-25587: Manipulim i Prototipit të Map

- **CVSS Score:** 10.0 (Kritike)
- **Vektori i sulmit:** Shfrytëzon një bug në implementimin `let` të bibliotekës
- **Mekanizmi i dobësisë:**
  - Targeton objektin `Map`, i listuar në `SAFE_PROTOTYPES`
  - Lejon mbishkrimin e metodës `Map.prototype.has`
  - Prototipi i `Map` mund të merret përmes `Map.prototype` për shkak të një defekti implementimi
- **Ndikimi:** Manipulim i logjikës së brendshme të sandbox-it, duke çuar në dalje nga izolimi

3. CVE-2026-25586: Ndotje e Prototipit të Host-it (Host Prototype Pollution)

- **CVSS Score:** 10.0 (Kritike)
- **Vektori i sulmit:** Shfrytëzon mekanizmin e kontrollit të pronave që përdor `hasOwnProperty`

- **Mekanizmi i dobësisë:**
  - Sulmuesit mund të "hijëzojnë" ose zëvendësojnë `hasOwnProperty` në objektet e sandbox-uara
  - Kur metoda e manipuluar kthen `true`, kontrollet e whitelist-it anashkalohen
  - Mundëson akses në prototipe sensitive, përfshirë `__proto__`
- **Ndikimi:** Anashkalim i plotë i mekanizmave të sigurisë, duke lejuar ndotje të ambientit host dhe ekzekutim arbitrar kodi

4. CVE-2026-25641: Gjendje Gare Time-of-Check to Time-of-Use (TOCTOU)

- **CVSS Score:** 10.0 (Kritike)
- **Vektori i sulmit:** Shfrytëzon hendekun kohor midis validimit të pronës dhe përdorimit të saj
- **Mekanizmi i dobësisë:**
  - Biblioteka validon çelësat e pronave në një moment, por i përdor më vonë pa ri-verifikim
  - Sulmuesit mund të dërgojnë objekte keqdashëse që shndërrohen në vlera string të ndryshme kur aksesohen
  - Çelësi i pronës duket i sigurt gjatë kontrollit të sigurisë, por transformohet në payload keqdashës gjatë aksesit real
- **Ndikimi:** Anashkalim i validimit të sigurisë dhe dalje nga sandbox-i

Versionet e Prekura

- **SandboxJS 0.8.28** dhe më herët

Versioni i Rregulluar

- **SandboxJS 0.8.29**

Rekomandime

AKSK rekomandon të**:**

- Identifikoni të gjitha sistemet, aplikacionet dhe ambientet që përdorin SandboxJS
- Përditësoni menjëherë të gjitha instalimet e SandboxJS në versionin 0.8.29 ose më të ri

Referenca

https://github.com/nyariv/SandboxJS/security/advisories/GHSA-58jh-xv4v-pcx4