مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Critical Vulnerabilities in SandboxJS

Tracking #:432318374

Date:09-02-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Four critical vulnerabilities have been identified in SandboxJS, a widely-used JavaScript sandbox library designed to isolate and secure the execution of untrusted code.

TECHNICAL DETAILS:

Four critical vulnerabilities have been identified in SandboxJS, a widely-used JavaScript sandbox library designed to isolate and secure the execution of untrusted code. All four vulnerabilities have been assigned the maximum Common Vulnerability Scoring System (CVSS) score of 10.0, indicating critical severity. These flaws allow attackers to completely bypass sandbox protections and execute arbitrary code on the host system, fundamentally compromising the security guarantees provided by the library.

VULNERABILITY DETAILS

1. **CVE-2026-25520: Function Return Value Exploitation**
   - CVSS Score: 10.0 (Critical)
   - Attack Vector: Exploits improper handling of function return values
   - Vulnerability Mechanism:
     - Return values of functions are not properly wrapped by the sandbox
     - Attackers can use Object.values or Object.entries to retrieve arrays containing the host's Function constructor
     - Provides direct access to the host execution environment
   - Impact: Complete sandbox escape with arbitrary code execution capabilities

2. **CVE-2026-25587: Map Prototype Manipulation**
   - CVSS Score: 10.0 (Critical)
   - Attack Vector: Exploits bug in the library's let implementation
   - Vulnerability Mechanism:
     - Targets the Map object, which is listed in SAFE_PROTOTYPES
     - Allows attackers to overwrite the Map.prototype.has method
     - Map prototype can be obtained via Map.prototype due to implementation flaw
   - Impact: Manipulation of sandbox internal logic leading to confinement escape

3. **CVE-2026-25586: Host Prototype Pollution**
   - CVSS Score: 10.0 (Critical)
   - Attack Vector: Exploits property checking mechanism using hasOwnProperty
   - Vulnerability Mechanism:
     - Attackers can "shadow" or replace hasOwnProperty on sandboxed objects
     - When the manipulated method returns true, whitelist security checks are bypassed
     - Enables access to sensitive prototypes including __proto__
   - Impact: Complete bypass of safety mechanisms, allowing host environment pollution and arbitrary code execution

4. **CVE-2026-25641: Time-of-Check to Time-of-Use (TOCTOU) Race Condition**
   - CVSS Score: 10.0 (Critical)
   - Attack Vector: Exploits timing gap between property validation and usage
   - Vulnerability Mechanism:
     - Library validates property keys at one point but uses them at another without re-verification
     - Attackers can pass malicious objects that coerce to different string values when accessed
     - Property key appears safe during security check but transforms into malicious payload during actual access
   - Impact: Bypass of security validation leading to sandbox escape

Affected Versions

- SandboxJS 0.8.28 and earlier

Remediated Version

- SandboxJS 0.8.29

RECOMMENDATIONS:

- Identify all systems, applications, and environments utilizing SandboxJS and Immediately upgrade all SandboxJS installations to fixed version or later.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

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