مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical SandboxJS Vulnerability Enables Remote Code Execution

Tracking #:432318610

Date:16-03-2026

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a critical security vulnerability (CVE-2026-26954) has been discovered in SandboxJS, a JavaScript sandboxing library used in web and Node.js environments to execute untrusted code safely.

TECHNICAL DETAILS:

A critical security vulnerability (CVE-2026-26954) has been discovered in SandboxJS, a JavaScript sandboxing library used in web and Node.js environments to execute untrusted code safely. The flaw allows attackers to escape the sandbox environment and execute arbitrary system commands on the host system. Successful exploitation could lead to **full remote code execution (RCE)**, enabling attackers to access sensitive data, run malicious commands, or compromise the affected server.

Vulnerability Information

- CVE ID: CVE-2026-26954
- Affected Software: SandboxJS
- Severity: Critical
- CVSS Score: 10.0
- Impact: Sandbox Escape leading to Remote Code Execution
- Affected Versions: ≤ 0.8.33
- Patched Version: 0.8.34

RECOMMENDATIONS:

- Organizations and developers should upgrade SandboxJS to fixed version or later immediately.

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-6r9f-759j-hjgv