مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerabilities in vm2 Node.js Sandbox Library

Tracking #:432318932

Date:11-05-2026

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 Multiple critical vulnerabilities in vm2, a widely used Node.js sandboxing library for executing untrusted JavaScript. These flaws allow attackers to bypass sandbox protections, escape isolation boundaries, and execute arbitrary code on host systems.

TECHNICAL DETAILS:

Vulnerability Details
Critical-Severity

- **CVE-2026-43997**
  - A code injection vulnerability allows attackers to obtain the host Object and fully escape the sandbox, leading to arbitrary code execution on the host system.
- **CVE-2026-44005**
  - A sandbox escape vulnerability enables attacker-controlled JavaScript to bypass isolation and trigger prototype pollution, potentially compromising application integrity and enabling arbitrary code execution.
- **CVE-2026-44006**
  - A code injection flaw in BaseHandler.getPrototypeOf allows attackers to break out of the sandbox and achieve remote code execution on the host.
- **CVE-2026-43999**
  - A NodeVM allowlist bypass vulnerability enables loading of restricted built-in modules such as child_process, allowing execution of arbitrary system commands.
- **CVE-2026-24118**
  - Sandbox escape via __lookupGetter__ permits arbitrary code execution on the host environment.
- **CVE-2026-24120**
  - A patch bypass for CVE-2023-37466 allows sandbox escape through the species property of Promise objects, leading to host command execution.
- **CVE-2026-24781**
  - Improper handling of the inspect function can be exploited to escape the sandbox and run arbitrary code.
- **CVE-2026-26332**
  - A flaw involving SuppressedError allows attackers to break sandbox restrictions and execute arbitrary commands.
- **CVE-2026-26956**
  - A protection mechanism failure triggered by Symbol-to-string coercion TypeError allows sandbox escape and arbitrary code execution.
- **CVE-2026-44008**
  - A sandbox escape via neutralizeArraySpeciesBatch() enables arbitrary command execution on the host.
- **CVE-2026-44009**
  - A null proto exception handling flaw enables sandbox escape and arbitrary command execution.
- **CVE-2026-44007**
  - An improper access control issue allows sandbox escape and execution of arbitrary operating system commands.

Fixed Versions

- vm2 version 3.11.2 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Vendor.

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/patriksimek/vm2/security/advisories