مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in jsPDF

Tracking #:432318211

Date:06-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical security vulnerability has been identified in jsPDF, a widely adopted JavaScript library used for PDF document generation.

TECHNICAL DETAILS:

A critical security vulnerability has been identified in jsPDF, a widely adopted JavaScript library used for PDF document generation. Tracked as CVE-2025-68428 and assigned a CVSS v4.0 score of 9.2 (Critical), the flaw allows unauthenticated remote attackers to read arbitrary files from the server's local file system when jsPDF is used in Node.js environments.
The vulnerability arises from improper input validation of file paths passed to multiple jsPDF methods. When exploited, sensitive files such as configuration secrets, credentials, or application data can be exfiltrated and embedded directly into generated PDF documents, resulting in severe confidentiality impact.

Vulnerability Details:

- CVE ID: CVE-2025-68428
- Affected Library: jsPDF (Node.js builds only)
- Severity: Critical
- CVSS v4.0 Score: 9.2 / 10
- Vulnerability Type:
  - Local File Inclusion (LFI)
  - Path Traversal
- Associated Weaknesses:
  - CWE-35 – Path Traversal
  - CWE-73 – External Control of File Name or Path

Affected & Patched Versions

- Vulnerable: jsPDF versions ≤ 3.0.4
- Patched: jsPDF version ≥ 4.0.0

Workarounds

- Use the Node.js *--permission* flag in production to restrict file system access and prevent unauthorized file reads.This feature is available from Node.js v20.0.0 and is stable for production use in v22.13.0, v23.5.0, and v24.0.0.

RECOMMENDATIONS:

- Organizations relying on jsPDF in Node.js environments should treat this issue as priority one and ensure upgrades or compensating controls are deployed without delay.

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/parallax/jsPDF/security/advisories/GHSA-f8cm-6447-x5h2