مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in sha.js JavaScript Library

Tracking #:432317627

Date:22-08-2025

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in sha.js, a widely used JavaScript library for cryptographic hashing. This flaw allows attackers to manipulate hash computations, potentially causing hash collisions, application crashes, or the exposure of cryptographic keys.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE ID**: CVE-2025-9288
- **Severity**: 9.1 Critical
- The vulnerability stems from missing input type checks, allowing attackers to manipulate hash computations. This can result in hash collisions, denial-of-service (DoS), and even private key extraction in cryptographic systems.

Impact:

Exploitation of this vulnerability can result in:

- Integrity compromise via hash collisions
- Application unavailability due to DoS
- Unauthorized recovery of cryptographic private keys

Affected Version:

- All versions prior to 2.4.12

Fixed Versions:

- 2.4.12 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed version released by the 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/browserify/sha.js/security/advisories/GHSA-95m3-7q98-8xr5