مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Critical Vulnerabilities in Deno Runtime

Tracking #:432318277

Date:20-01-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that two significant security vulnerabilities have been identified in Deno, the modern JavaScript and TypeScript runtime.

TECHNICAL DETAILS:

Two significant security vulnerabilities have been identified in Deno, the modern JavaScript and TypeScript runtime known for its secure-by-default design. The flaws affect Deno's Node.js compatibility layer and Windows command execution safeguards, undermining core security guarantees.

Vulnerability 1: Improper Cipher Finalization in node:crypto

- CVE ID: CVE-2026-22863
- Severity: Critical
- CVSS Score: 9.2
- Affected Component: node:crypto compatibility layer
- Impact: Cryptographic state leakage, exposure of server secrets

Vulnerability 2: Windows Command Execution Bypass

- CVE ID: CVE-2026-22864
- Severity: High
- Affected Component: Deno.Command API (Windows)
- Impact: Arbitrary code execution

Affected Versions

- All Deno versions prior to v2.6.0

Fixed Versions

- Upgrade Deno to version 2.6.0 or later

RECOMMENDATIONS:

- Upgrade Deno 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://nvd.nist.gov/vuln/detail/CVE-2026-22863
- https://nvd.nist.gov/vuln/detail/CVE-2026-22864