مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical RCE Vulnerability in NestJS Devtools Integration

Tracking #:432317564
Date:04-08-2025

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

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical remote code execution (RCE) vulnerability, in the @nestjs/devtools-integration package of the popular NestJS framework. This flaw allows attackers to execute arbitrary code on developer machines with minimal user interaction, posing a severe risk of system compromise.

TECHNICAL DETAILS:

A critical remote code execution (RCE) vulnerability has been identified in the @nestjs/devtools-integration package of the widely-used NestJS framework. Tracked as CVE-2025-54782, this flaw allows attackers to execute arbitrary JavaScript code on developer machines during development. Exploitation may result in complete system compromise simply by visiting a malicious webpage.

Vulnerability Details:

- CVE ID CVE-2025-54782
- CVSS v4 Score 9.4 Critical
- The vulnerability resides in the /inspector/graph/interact endpoint exposed by the devtools package when enabled. This endpoint executes JavaScript code using an insecure sandbox modeled after the deprecated safe-eval library, leveraging Node.js's vm.runInNewContext()—a method explicitly not intended for executing untrusted code.
- Additionally, the endpoint fails to validate critical cross-origin request headers (e.g., Origin, Content-Type) and sets a static Access-Control-Allow-Origin header, enabling cross-origin requests from malicious sites.
- Exploitation of this vulnerability can lead to remote code execution, data exfiltration, malware deployment, or full system compromise.

Affected versions

- <=0.2.0

Fixed Versions

- 0.2.1 or later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the fixed or latest updates 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://nvd.nist.gov/vuln/detail/CVE-2025-54782