مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Angular framework

Tracking #:432318622

Date:18-03-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in the Angular framework that can bypass built-in protections, potentially leading to Cross-Site Scripting (XSS) attacks.

TECHNICAL DETAILS:

A significant security vulnerability has been identified in the Angular framework affecting its runtime and compiler components. The flaw allows attackers to bypass Angular's built-in sanitization protections, potentially leading to Cross-Site Scripting (XSS) attacks. This issue arises from improper handling of internationalization (i18n) attributes and poses a high risk to applications processing untrusted user input.

Vulnerability Details

- **CVE ID:** CVE-2026-32635
- **Severity:** High **CVSS Score:** 8.6
- A Cross-Site Scripting (XSS) vulnerability exists in the Angular runtime and compiler. It occurs when a security-sensitive attribute (e.g., href) is marked for internationalization using i18n-. This bypasses Angular's built-in sanitization, and when untrusted data is bound to the attribute, an attacker can inject and execute malicious scripts.
- Successful exploitation of this vulnerability may lead to:
  - Session Hijacking: Theft of session cookies and authentication tokens
  - Data Exfiltration: Unauthorized access and transmission of sensitive user data
  - Unauthorized Actions: Execution of actions on behalf of authenticated users

Affected Products

- Applications using vulnerable versions of the Angular framework (runtime and compiler)

Fixed Versions

- 22.0.0-next.3
- 21.2.4
- 20.3.18
- 19.2.20

RECOMMENDATIONS:

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

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://www.cve.org/CVERecord?id=CVE-2026-32635