مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Notepad++

Tracking #:432318854

Date:28-04-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in Notepad++ that allows attackers to trigger application crashes or expose sensitive memory information through maliciously crafted localization files.

TECHNICAL DETAILS:

Vulnerability Details

CVE-2026-3008 – Format String Injection in Notepad++ nativeLang.xml Parsing

- **Severity:** Critical | **CVSS v4:** 10
- The vulnerability exists in Notepad++'s improper handling of the find-result-hits parameter within the nativeLang.xml language configuration file. When users execute "Find ALL in Current Document" or related search operations, specially crafted format string payloads embedded in this XML file are processed without sufficient validation.
- Successful exploitation of this vulnerability may allow an attacker to cause application instability or crashes, potentially resulting in a denial-of-service condition. It may also lead to the disclosure of sensitive memory contents, which could expose internal application data and assist in further exploitation attempts or weakening of system security protections.

Affected Version

- Notepad++ version 8.9.3

Fixed Version

- Notepad++ version 8.9.4 or later

RECOMMENDATIONS:

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

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.tenable.com/cve/CVE-2026-3008