مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Multiple Vulnerabilities in Libxml2

Tracking #:432316898

Date: 24-02-2025

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

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed multiple vulnerabilities in Libxml2 that can lead to denial of service, application crashes, or arbitrary code execution on affected systems.

TECHNICAL DETAILS:

Libxml2, a widely used XML parsing library developed for the GNOME project and utilized across various platforms, including Linux, Windows, macOS, and Unix-based systems, has been found to contain multiple vulnerabilities.

Vulnerability Details:
CVE-2024-56171 (CVSS 7.8) - Use-After-Free Vulnerability

- A use-after-free vulnerability exists in the xmlSchemaIDCFillNodeTables and xmlSchemaBubbleIDCNodeTables functions.
- Exploitation can occur through the processing of specially crafted XML documents or schemas.
- Successful exploitation may lead to arbitrary code execution.

CVE-2025-24928 (CVSS 7.8) - Stack-Based Buffer Overflow

- A stack-based buffer overflow vulnerability has been discovered in the xmlSnprintfElements function.
- This issue can be triggered during DTD validation of untrusted XML documents or DTDs.
- Exploitation may result in denial of service or arbitrary code execution.

CVE-2025-27113 (CVSS 2.9) - NULL Pointer Dereference

- A NULL pointer dereference vulnerability exists in the xmlPatMatch function.
- This vulnerability can be triggered under specific conditions, such as:
    - Using the Perl module XML::LibXML::Reader with certain options.
    - Running the xmllint tool with specific flags.
- Successful exploitation may lead to application crashes but is unlikely to lead to remote code execution.

Affected Versions:

- Libxml2 prior to **2.12.10** and **2.13.6**.

Fixed Versions:

- Libxml2 **2.12.10** or **2.13.6 or** later

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Libxml2.

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-2024-56171
- https://nvd.nist.gov/vuln/detail/CVE-2025-24928
- https://nvd.nist.gov/vuln/detail/CVE-2025-27113