مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in libxml2

Tracking #:432316681

Date:27-12-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in libxml2, a widely-used XML parsing library. This flaw allows attackers to compromise systems and steal sensitive data, posing a significant threat to various applications and environments that rely on libxml2.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-40896**
- CVSS score 9.1 (Critical)
- The vulnerability resides in libxml2's SAX parser, which can produce events for external entities even when custom SAX handlers attempt to override entity content. This oversight allows attackers to launch classic XML External Entity (XXE) attacks, potentially compromising systems and stealing sensitive data.
- Successful exploitation of this vulnerability could lead to:
  - Unauthorized access to sensitive information
  - Remote Code Execution (RCE) in misconfigured environments
  - Denial of Service (DoS) attacks
  - Attackers can potentially access local files (e.g., /etc/passwd), execute commands, and exhaust system resources

Affected Versions:

- 2.11 before 2.11.9
- 2.12 before 2.12.9
- 2.13 before 2.13.3

Fixed Versions:

- libxml2 2.11.9, 2.12.9, or 2.13.3

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to upgrade the affected versions to the fixed versions at the earliest.

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-2024-40896