مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Remote Code Execution Vulnerability in libssh2

Tracking #:432319188

Date:24-06-2026

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in libssh2 that could allow remote attackers to cause memory corruption and potentially achieve remote code execution on vulnerable systems.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2026-55200**
  Severity: Critical | **CVSS:** 9.2 (CVSS v4)
- An out-of-bounds write vulnerability exists in the ssh2_transport_read() function due to insufficient validation of the packet_length field. A remote attacker can send a specially crafted SSH packet with an excessively large packet length value, resulting in heap memory corruption and potential remote code execution.

Affected Products and Versions

- libssh2 version 1.11.1 and earlier

Fixed Version

- Update to a version containing patch commit 7acf3df

RECOMMENDATIONS:

- Apply the latest security updates for libssh2 and affected applications.
- Identify and remediate vulnerable instances across the environment.
- Monitor systems for abnormal SSH-related activity or application crashes.
- Maintain an inventory of third-party libraries and dependencies to facilitate timely patching.
- Follow vendor security advisories and update guidance.

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-2026-55200