مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High Severity Vulnerability in libssh2 Publickey Subsystem

Tracking #:432319205

Date:28-06-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity heap buffer overflow vulnerability has been publicly disclosed in libssh2, an open-source client-side SSH library widely used by file transfer applications, automation tools, embedded devices, and programming language bindings.

TECHNICAL DETAILS:

A high-severity heap buffer overflow vulnerability, CVE-2026-58050, has been publicly disclosed in libssh2, an open-source client-side SSH library widely used by file transfer applications, automation tools, embedded devices, and programming language bindings.
The vulnerability affects libssh2 versions 1.11.1 and earlier and resides within the publickey subsystem. A malicious or compromised SSH server can exploit the flaw by sending a specially crafted response that triggers an integer overflow during memory allocation, resulting in heap corruption. Public proof-of-concept (PoC) exploit code has been released, demonstrating potential remote code execution on affected Windows systems.
Although there is no evidence of active exploitation in the wild, the public availability of exploit code significantly increases the likelihood of future attacks. Organizations using libssh2 should prioritize updating to a fixed release as soon as it becomes available and implement temporary mitigation measures where patching is not immediately possible.

Vulnerability Details:

- CVE ID: CVE-2026-58050
- Severity: High
- CVSS v4 Score: 8.3
- Affected Product: libssh2
- Affected Versions: All versions up to and including 1.11.1
- Vulnerability Type: Heap Buffer Overflow caused by an Integer Overflow
- CWE: CWE-190 – Integer Overflow or Wraparound
- Affected Component: Publickey subsystem attribute parser
- Attack Vector: Network (malicious or compromised SSH server)
- Attack Prerequisites: A client must connect to a malicious SSH server or a server controlled by a Man-in-the-Middle (MitM) attacker.
- Root Cause: Insufficient validation of a server-supplied 32-bit attribute count results in an integer overflow during memory allocation on 32-bit platforms.
- Impact: Heap memory corruption that may lead to application crashes (Denial of Service) or potential Remote Code Execution (RCE).
- Exploitation Status: Public proof-of-concept (PoC) exploit code is available; no confirmed in-the-wild exploitation has been reported.
- Primary Affected Platforms: 32-bit systems are most susceptible due to integer wraparound during buffer size calculation.

RECOMMENDATIONS:

Immediate Actions:

- Upgrade to a patched version of libssh2 as soon as it becomes available and restrict SSH connections to trusted hosts until remediation is complete.

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-2026-58050