Date Posted: 2026/02/06

[Vulnerability Alert] Critical Security Vulnerability Found in OpenSSL Library (CVE-2025-15467)

- Subject Explanation: [Vulnerability Alert] Critical Security Vulnerability Found in OpenSSL Library (CVE-2025-15467)
- Content Description:
  - Forwarding Taiwan Computer Emergency Response Team / Coordination Center (TWCERT/CC) Security Alert TWCERTCC-200-202601-00000029
  - OpenSSL is an open-source encryption library primarily used for secure communication, SSL/TLS protocol implementation, and certificate management. It supports various encryption algorithms and is widely used in servers and applications.
  - Recently, OpenSSL released a security update to patch a critical security vulnerability (CVE-2025-15467, CVSS: 9.8). This is a heap buffer overflow vulnerability that may cause the program to terminate abnormally, triggering a Denial of Service (DoS) attack, or even potentially causing remote code execution.
- Impacted Platforms:
  - OpenSSL library versions from 3.6.0 to prior to 3.6.1
  - OpenSSL library versions from 3.5.0 to prior to 3.5.5
  - OpenSSL library versions from 3.4.0 to prior to 3.4.4
  - OpenSSL library versions from 3.3.0 to prior to 3.3.6
  - OpenSSL library versions from 3.0.0 to prior to 3.0.19
- Suggested Measures:
  - Please update to the following versions: OpenSSL library 3.6.1 (or later), OpenSSL library 3.5.5 (or later), OpenSSL library 3.4.4 (or later), OpenSSL library 3.3.6 (or later), OpenSSL library 3.0.19 (or later)
- References:
  1. https://www.twcert.org.tw/tw/cp-169-10692-38c40-1.html

Computer and Communication Center Network Systems Division