مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

RCE Vulnerability in ExifTool

Tracking #:432319003

Date:20-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a high severity vulnerability has been identified in ExifTool, tracked as CVE-2026-3102, which allows attackers to execute arbitrary commands on macOS systems through specially crafted image metadata.

TECHNICAL DETAILS:

A high severity vulnerability has been identified in ExifTool, tracked as CVE-2026-3102, which allows attackers to execute arbitrary commands on macOS systems through specially crafted image metadata. The flaw affects ExifTool version 13.49 and earlier and is caused by improper sanitization of metadata fields during command execution. Attackers can exploit the issue by embedding malicious payloads into image metadata fields and triggering vulnerable processing workflows using specific ExifTool options.

Vulnerability Details

- CVE ID: CVE-2026-3102
- Severity: 8.8 HIGH
- Affected Software: ExifTool
- Affected Versions: 13.49 and earlier
- Fixed Version: 13.50
- Vulnerability Type: Command Injection / Remote Code Execution (RCE)
- Attack Vector: Malicious image metadata
- Target Platform: macOS

RECOMMENDATIONS:

- Update immediately ExifTool to fixed version.

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://github.com/exiftool/exiftool/releases/tag/13.50