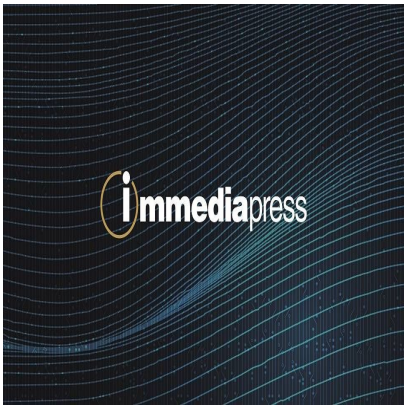

Kaspersky GReAT scopre una vulnerabilitÃ di tipo command injection in ExifTool che interessa gli utenti MacOS

Descrizione

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

Una vulnerabilitÃ in uno strumento open source per la gestione dei metadati, ampiamente utilizzato, consente lâ??esecuzione di codice arbitrario tramite file immagine appositamente creati; Ã¨ giÃ disponibile una patch.

Il Global Research and Analysis Team (GReAT) di Kaspersky ha individuato una vulnerabilitÃ di tipo command injection (CVE-2026-3102) in ExifTool, uno strumento gratuito e open source utilizzato in tutto il mondo per leggere e modificare i metadati di immagini, video e file PDF. La falla, che interessa i sistemi MacOS che eseguono ExifTool versione 13.49 e precedenti, potrebbe consentire a un aggressore di eseguire comandi arbitrari incorporando istruzioni nascoste nei metadati di un file immagine. Il responsabile del progetto, Phil Harvey, ha corretto la vulnerabilitÃ nella versione 13.50 di ExifTool, rilasciata il 7 febbraio.

La vulnerabilitÃ deriva da una sanificazione impropria degli input nel modo in cui ExifTool elabora determinati tag di metadati su MacOS. Un aggressore puÃ² creare un file PNG dannoso contenente comandi incorporati che vengono eseguiti quando ExifTool elabora il file. Lâ??exploit Ã¨ di bassa complessitÃ : un comando genera lâ??immagine compromessa e un secondo comando ne attiva lâ??esecuzione sul sistema di destinazione.

Una volta sfruttata, la vulnerabilitÃ potrebbe consentire a un malintenzionato di scaricare ed eseguire ulteriori payload malware o di raccogliere informazioni sensibili dai file, incluse immagini e PDF, archiviati sul computer compromesso.

ExifTool Ã¨ un programma software gratuito e open source per la lettura, la scrittura e la manipolazione dei metadati di immagini, audio, video e PDF. Ã? comunemente integrato in diversi tipi di workflow digitali ed Ã¨ spesso utilizzato nellâ??analisi forense digitale e nellâ??archiviazione di library. I tipici pivot OSINT includono lâ??estrazione di date e luoghi di acquisizione, lâ??identificazione del software di editing, la riconciliazione dei file sidecar e il confronto dei delta dei metadati tra diverse versioni.

â??Quello che rende questa vulnerabilitÃ particolarmente rilevante Ã¨ il contrasto tra la semplicitÃ con cui puÃ² essere sfruttata utilizzando determinate righe di comando e la profonda integrazione di ExifTool nei flussi di lavoro professionali. Chiunque utilizzi ExifTool su MacOS dovrebbe aggiornarlo alla versione 13.50, mentre i team che impiegano pipeline automatizzate dovrebbero verificare anche quale versione viene richiamata dai propri scriptâ?•, ha dichiarato Lucas Tay, Security Researcher di Kaspersky GReAT.

Per mitigare CVE-2026-3102, Kaspersky raccomanda di:

Le aziende che utilizzano componenti open source nei propri flussi di lavoro possono avvalersi di Kaspersky Open Source Software Threats Data Feed per monitorare costantemente le vulnerabilitÃ lungo lâ??intera catena di fornitura del software.

Contatti:
Kaspersky
kaspersky@noesis.net

COMUNICATO STAMPA â?? CONTENUTO PROMOZIONALE

ResponsabilitÃ editoriale di Kaspersky

â??

immediapress

Categoria

1. Comunicati

Tag

1. ImmediaPress

Data di creazione
Febbraio 25, 2026

Autore
redazione