ESET Research analyzed a critical flaw in Windows Imaging Component, which abuses JPG files

DUBAI , DUBAI, UNITED ARAB EMIRATES, December 24, 2025 /EINPresswire.com/ -- ESET researchers have examined CVE-2025-50165, a serious Windows vulnerability that theoretically grants remote code execution by opening a specially crafted JPG file – one of the most widely used image formats. ESET's root cause analysis pinpoints the exact location of the faulty code and reproduces the crash. However, ESET Research believes that the exploitation scenario is harder than it appears to be. The flaw was found and documented by Zscaler ThreatLabz and has already been patched by Microsoft, in August.

"WindowsCodecs.dll crashes when attempting to encode a JPG image with 12-bit or 16-bit data precision. Although Microsoft has classified this vulnerability as critical, our in-depth analysis indicates that large-scale exploitation is highly improbable," says ESET researcher Romain Dumont, who investigated the vulnerability. "Simply opening, and therefore decoding and rendering, a specially crafted image will not trigger the vulnerability. However, the vulnerable function jpeg_finish_compress could be called if the image is saved or if a host application, such as the Microsoft Photos application, creates thumbnails of images," explains Dumont.

CVE-2025-50165 is a flaw in the encoding and compressing process of a JPG image, not in its decoding. ESET provides both its own method to reproduce the crash using a simple 12-bit or 16-bit JPG image, and an examination of the initial released patch. Furthermore, the investigation revealed that the vulnerable component uses the open-source library libjpeg-turbo, in which similar issues were found and resolved in December 2024.

Although JPG is older, widely used, and perhaps the most popular digital image format in automated software testing, vulnerabilities can still be found in some codecs. This ESET Research study of CVE-2025-50165 also highlights the importance of keeping up with security updates

when using third-party libraries. As WindowsCodecs.dll is a library, a host application would be considered vulnerable if it allows JPG images to be (re-)encoded, and exploitable only if an attacker has enough control over the application (address leak, heap manipulation).

For a more detailed analysis of the CVE 2025 50165 vulnerability, check out the latest ESET Research blogpost "Revisiting CVE-2025-50165: A critical flaw in Windows Imaging Component" on WeLiveSecurity.com. Make sure to follow ESET Research on Twitter (today known as X), BlueSky, and Mastodon for the latest news from ESET Research.

About ESET
ESET® provides cutting-edge cybersecurity to prevent attacks before they happen. By combining the power of AI and human expertise, ESET stays ahead of emerging global cyberthreats, both known and unknown—securing businesses, critical infrastructure, and individuals. Whether it's endpoint, cloud, or mobile protection, our AI-native, cloud-first solutions and services remain highly effective and easy to use. ESET technology includes robust detection and response, ultra-secure encryption, and multifactor authentication. With 24/7 real-time defense and strong local support, we keep users safe and businesses running without interruption. The ever-evolving digital landscape demands a progressive approach to security: ESET is committed to world-class research and powerful threat intelligence, backed by R&D centers and a strong global partner network. For more information, visit ESET Middle East or follow us on LinkedIn, Facebook & X.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here