Trinity Cyber

Case Study

Preventing WebP Exploitation (CVE-2023-4863)

Executive Summary

Trinity Cyber has developed a unique way to detect and prevent exploitation of a high-profile and widespread WebP image vulnerability (CVE-2023-4863) for all customers.

This vulnerability is complex and cannot be detected with traditional pattern-matching signature logic. The core engine behind Trinity Cyber now harnesses logic for checking the heap overflow condition found in malicious WebP images with altered Huffman coding tables; **allowing precise targeting and removal of these images by finding actual heap overflows within them.**

Technical Details

WebP is an open-source image format developed by Google with the goal of reducing image file sizes compared to older image formats like GIF, JPEG and PNG. The library behind the WebP format (called 'libwebp') is widely used by third-party developer projects that handle or generate WebP files. This library enables ease of use and integration of WebP files. With support for WebP format in all modern web browsers (Chrome, Firefox, MS Edge, Safari) and major operating systems (Windows, MacOS, Linux), it also exposes a very large attack surface.

CVE-2023-4863 is a heap overflow in the libwebp library that can lead to Remote Code Execution (RCE) via crafted WebP files. The vulnerability was disclosed by Citizen Lab while investigating BLASTPASS attacks against iOS devices as part of a 'zero click' chain developed by NSO group. Briefly, this CVE was labeled as CVE-2023-5129 and classified as a CVSS 10, however this CVE was rejected as a duplicate, leaving CVE-2023-4863 with a CVSS score of 8.8. At the time of this writing an upstream patch has been introduced to the 'libwebp' library to fix the vulnerability, but it may take months before broad adoption of this patch reaches vulnerable devices.

The heap buffer overflow can be found in the lossless compression capability of 'libwebp' as it relates to processing Huffman coding tables. Essentially, an attacker can control data in the second level Huffman coding tables of a crafted WebP image to achieve an Out of Bounds (OOB) write of malicious data via the ReplicateValue operation. Current Proof of Concept (POC) code demonstrates this, and exploitation via the BLASTPASS campaign has been observed in the wild.

Evolving Protection

When initial POCs released in late September, Trinity Cyber developed countermeasures against known POCs with information available. In the fight against adversaries, good enough is never good enough, so the team set out to introduce a more holistic ability to detect WebP heap overflows used in CVE-2023-4863 to better protect our customers. During this effort, inspiration from various sources including the actual vulnerable code was drawn. Within 48 hours our Engineering team had introduced a major capability improvement to the core engine which allowed our Analysis teams to harness a simple boolean (true/false) value to detect the actual conditions of the attack. Because of this, our detection logic became shorter and more concise while enabling greater coverage of the conditions that cause heap overflows in Huffman coding tables. This collaboration between Engineering and Analysis teams is one of the cornerstones on which Trinity Cyber's managed services are offered.

Trinity Cyber released holistic protection for all customers against CVE-2023-4863 on October 03, 2023 that does not depend on ephemeral signatures, IOCs, or domains where adveraries may stage malicious WebP attacks. As the WebP situation evolves, Trinity Cyber will continue to prevent attacks against users and devices in both **TC:Edge** and **TC:File** services.

About Trinity Cyber

Trinity Cyber is an international cybersecurity firm that invents and operates innovative solutions to the most difficult cybersecurity challenges. The company's products and services replace multiple market segments in the traditional cybersecurity market, with customers in over a dozen of the largest market verticals. The company's founders, management team, and technologists are all award-winning, recognized leaders in their field—and their tech has revolutionized network security.

Contact Us

For more information, please feel free to reach out to our sales or customer success teams at sales@trinitycyber.com