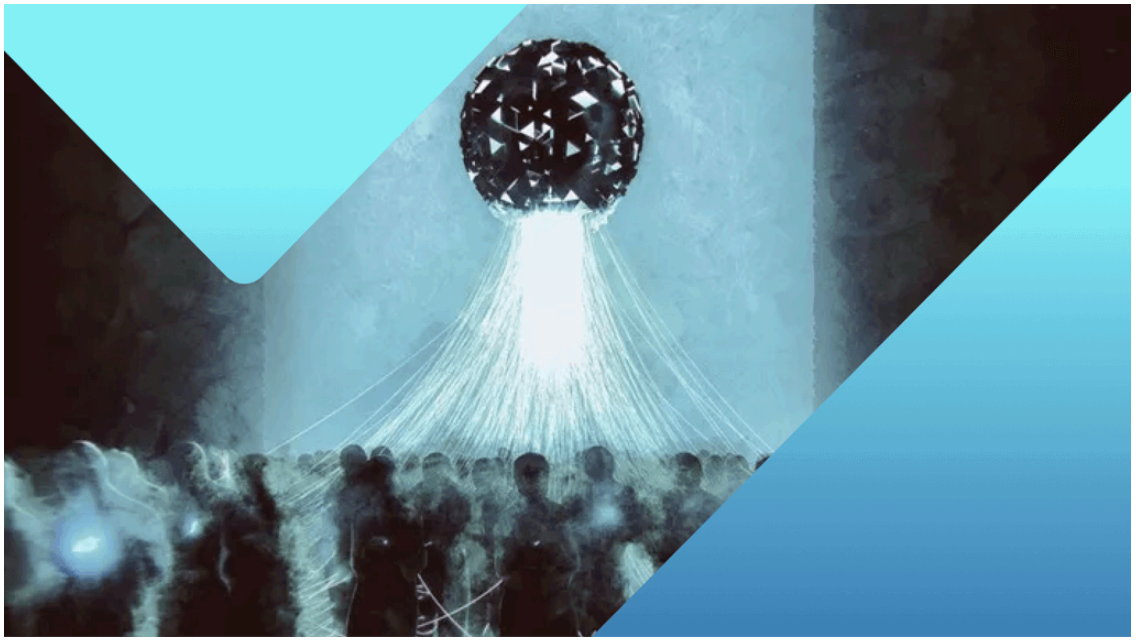
Pegasus spyware and how it exploited a WebP vulnerability

By Pieter Arntz

Published: 2023-09-27 · Archived: 2026-04-06 00:35:05 UTC



September 27, 2023

Recent events have demonstrated very clearly just how persistent and wide-spread the Pegasus spyware is. For those that have missed the subtle clues, we have tried to construct a clear picture. We attempted to follow the timeline of events, but have made some adjustments to keep the flow of the story alive.

On September 12, 2023 we published two blogs urging our readers to urgently patch two Apple issues which were added to the catalog of known exploited vulnerabilities by the Cybersecurity & Infrastructure Security Agency (CISA), and to apply an update for Chrome that included one critical security fix for an actively exploited vulnerability.

The vulnerabilities were discovered as zero-days by CitizenLab, while checking the device of an individual employed by a Washington DC-based civil society organization with international offices. The exploit chain based on these vulnerabilities was capable of compromising devices without any interaction from the victim and were reportedly used by the NSO Group to deliver its infamous Pegasus spyware.

Both of the vulnerabilities, CVE-2023-41064 and CVE-2023-4863 were based on a heap buffer overflow in Libwebp, the code library used to encode and decode images in the WebP format. This library can be used in other programs, such as web browsers, to add WebP support.

Security expert Ben Hawkes figured out that the vulnerability was to be found in the “lossless compression” support for WebP, sometimes known as VP8L. A lossless image format can store and restore pixels with 100%

accuracy, and WebP does this using an algorithm called Huffman coding.

As we saw in the vulnerability descriptions, both vulnerabilities were buffer overflow issues. A buffer overflow is a type of software vulnerability that exists when an area of memory within a software application reaches its address boundary and writes into an adjacent memory region.

The vulnerable versions of libwebp use memory allocations based on pre-calculated buffer sizes from a fixed table, and then construct the necessary Huffman tables directly into that allocation. By creating specially crafted image files that tricked libwebp into creating tables that were too small to contain all the values, the data would overflow into other memory locations.

Even a weathered security expert like Ben Hawkes, who figured out where the problem was, had a hard time finding a way to exploit this issue. Let alone how hard it must have been when there was no clue that a vulnerability even existed. It helps that libwebp is an open source library, so anyone interested can review the code. Ben explained that even extensive fuzzing had never revealed the problem.

Someone, or a group of people, must have taken it upon themselves to really dive into the code. Ben wrote:

> "In practice, I suspect this bug was discovered through manual code review. In reviewing the code, you would see the huffman_tables allocation being made during header parsing of a VP8L file, so naturally you would look to see how it's used. You would then try to rationalize the lack of bounds checks on the huffman_tables allocation, and if you're persistent enough, you would progressively go deeper and deeper into the problem before realizing that the code was subtly broken. I suspect that most code auditors aren't that persistent though — this Huffman code stuff is mind bending — so I'm impressed."

Then again, seeing the amount of money that one could cash in for a fully functional exploit chain, there should be more than enough people willing to put in the work and shove their conscience aside.

20 million dollar for top-tier full-chain mobile exploits

And although Google and Apple have issued updates to patch this vulnerability, libwebp is used in many other applications. And it may take a while before the Android update trickles down to every make and model. Regular readers may know that when there is an update for the Android operating system—software that sits at the core of about 70% of all mobile devices—it can take a very long time to reach end users due to a patch gap. This is because many mobile phone vendors sell their devices with their own tweaked versions of Android and the patches need to be tested before they can be rolled out on those versions.

The NSO group that markets the Pegasus spyware have shown they are interested in acquiring such exploits. As we wrote years ago, the Pegasus spyware has been around for years and we should not ignore its existence.

Our own David Ruiz wrote:

> "Pegasus is reportedly instrumental to several governments' oppressive surveillance campaigns against their own citizens and residents, and, while NSO Group has repeatedly denied allegations that it complicity sells Pegasus to human right abusers, it is difficult to reconcile exactly how the zero-click spyware program—which non-consensually and invisibly steals emails, text messages, photos, videos, locations, passwords, and social media activity—is at the same time a tool that can, in its very use, respect the rights of those around the world to speak freely, associate safely, and live privately."

Pegasus is not new. The company behind it launched in 2010, and it reportedly gained its first overseas customer just one year later. For years, Citizen Lab has been tracking the spread of Pegasus, searching for government clients and tracking down mobile devices that were hacked by the spyware. Back in 2016, the group's investigations helped spur MacOS updates to fix severe vulnerabilities that could have been exploited by Pegasus. In 2018, Citizen Lab also identified 45 countries that were potentially relying on Pegasus to conduct surveillance.

After learning about the findings from The Pegasus Project, former NSA defense contractor and surveillance whistleblower Edward Snowden warned that spyware is not a small problem. It is, he said, everywhere.

> "When I look at this, what the Pegasus Project has revealed is a sector where the only product are infection vectors, right? They don't—they're not security products. They're not providing any kind of protection, any kind of prophylactic."

Snowden said.

> "They don't make vaccines. The only thing they sell is the virus."
