

Researcher Turns Insecure License Plate Cameras Into Open Source Surveillance Tool

Jason Koebler : 6-7 minutes : 1/7/2025

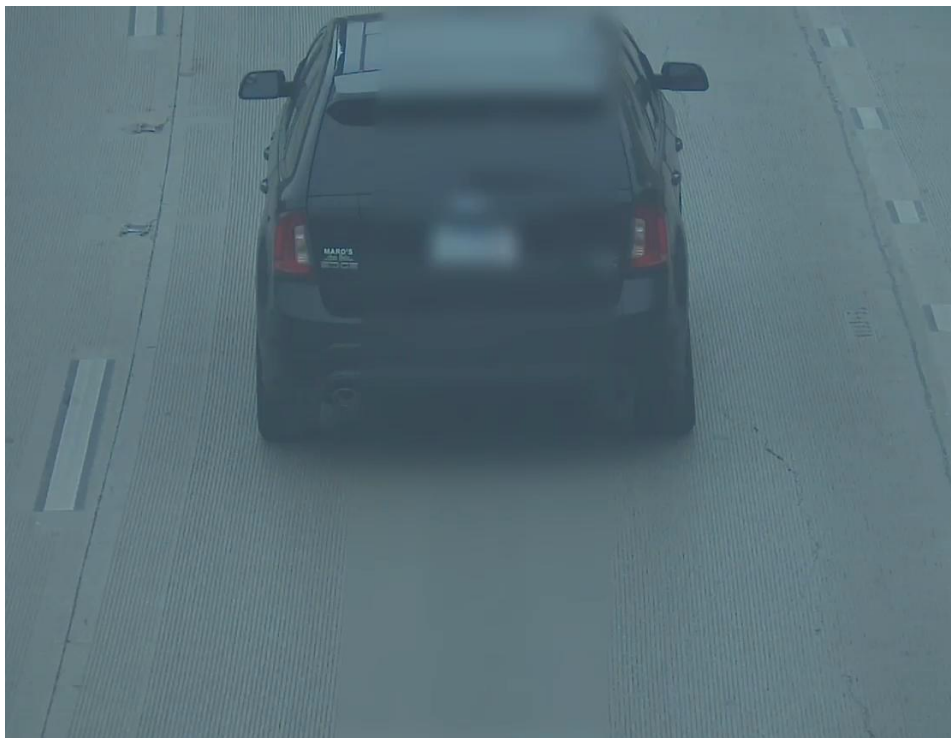
Some Motorola automated license plate reader surveillance cameras are live-streaming video and car data to the unsecured internet where anyone can watch and scrape them, a security researcher has found. In a proof-of-concept, a privacy advocate then developed a tool that automatically scans the exposed footage for license plates, and dumps that information into a spreadsheet, allowing someone to track the movements of others in real time.

Matt Brown of Brown Fine Security made a [series](#) of YouTube videos showing vulnerabilities in a Motorola Reaper HD ALPR that he bought on eBay. As we [have reported previously](#), these ALPRs are deployed all over the United States by cities and police departments. Brown initially found that it is possible to view the video and data that these cameras are collecting [if you join the private networks that they are operating on](#). But then he found that many of them are misconfigured to stream to the open internet rather than a private network.

“My initial videos were showing that if you’re on the same network, you can access the video stream without authentication,” Brown told 404 Media in a video chat. “But then I asked the question: What if somebody misconfigured this and instead of it being on a private network, some of these found their way onto the public internet?”

In his most recent video, Brown shows that many of these cameras are indeed misconfigured to stream both video as well as the data they are collecting to the open internet and whose IP addresses can be found using the Internet of Things search engine Censys. The streams can be watched without any sort of login.

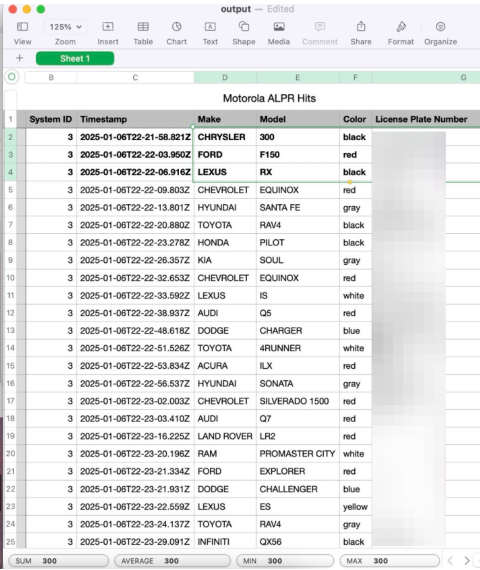
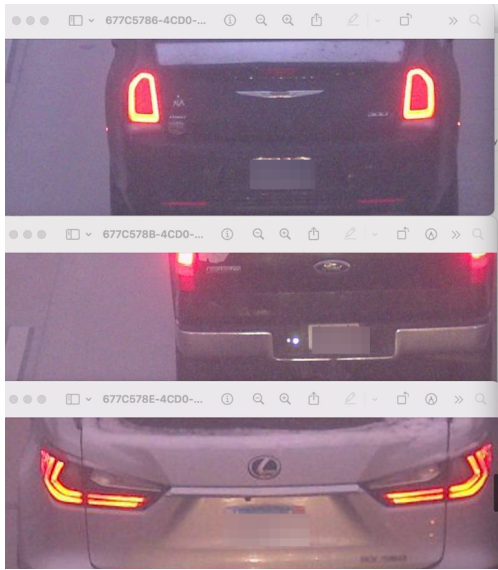
In many cases, they are streaming color video as well as infrared black-and-white video of the streets they are surveilling, and are broadcasting that data, including license plate information, onto the internet in real time.

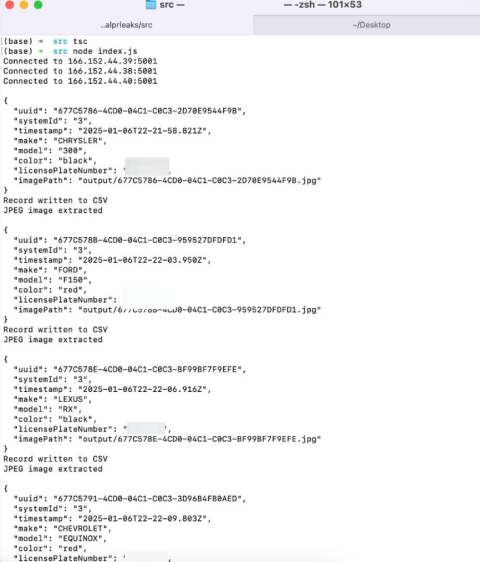
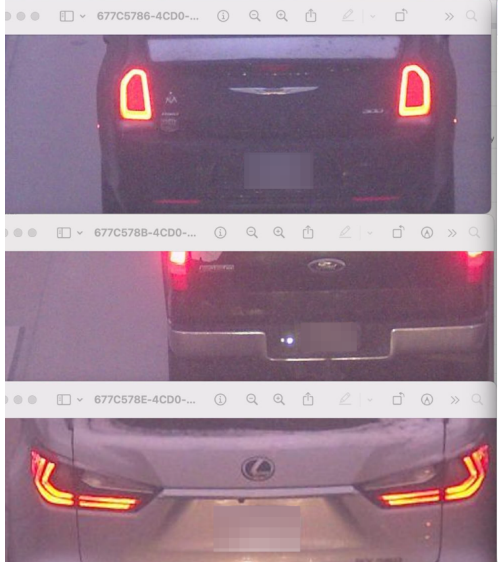


Will Freeman, [the creator of DeFlock](#), an open-source map of ALPRs in the United States, said that people in the DeFlock community have found many ALPRs that are streaming to the open internet. Freeman built a proof of concept script that takes data from unencrypted Motorola ALPR streams, decodes that data, and adds timestamped information about specific car movements into a spreadsheet. A spreadsheet he sent me shows a car’s make, model, color, and license plate number associated with the specific time that they drove past an

unencrypted ALPR near Chicago. So far, roughly 170 unencrypted ALPR streams have been found.

“Let’s say 10 of them are in a city at strategic locations. If you connect to all 10 of them, you’d be able to track regular movements of people,” Freeman said.





Freeman told 404 Media that this fact is more evidence that the proliferation of ALPRs around the United States and the world represents a significant privacy risk, and Freeman has been a strong advocate against the widespread adoption of ALPRs.

“I’ve always thought these things were concerning, but this just goes to show that law enforcement agencies and the companies that provide ALPRs are no different than any other data company and can’t be trusted with this information,” Freeman told 404 Media. “So when a police department says there’s nothing to worry about unless you’re a criminal, there definitely is. Here’s evidence of a ton of cameras operated by law enforcement freely streaming sensitive data they’re collecting on us. My hometown is mostly Motorola [ALPRs], so someone could simply write a script that maps vehicles to times and precise locations.”

A Motorola Solutions spokesperson told 404 Media that the company is working on a firmware update that “will introduce additional security hardening.”

“Motorola Solutions designs, develops and deploys our products to prioritize data security and protect the confidentiality, integrity and availability of data,” the spokesperson said. “The ReaperHD camera is a legacy device, sales of which were discontinued in June 2022. Findings in the recent YouTube videos do not pose a risk to customers using their devices in accordance with our recommended configurations. Some customer-modified network configurations potentially exposed certain IP addresses. We are working directly with these customers to restore their system configurations consistent with our recommendations and industry best practices. Our next

firmware update will introduce additional security hardening.”

This is not the first time that ALPRs have been found to be streaming [directly to the unsecured internet](#). In 2015, the [Electronic Frontier Foundation](#) and researchers at the University of Arizona found hundreds of exposed ALPR streams. In 2019, an ALPR vendor for the Department of Homeland Security [was hacked and license plates and images of travelers](#) were leaked onto the dark web. Last year, the U.S. government’s Cybersecurity and Infrastructure Security Agency put out a warning saying that [Motorola’s Vigilant ALPR cameras](#) were remotely exploitable.

Brown said that, although not all Motorola ALPRs are streaming to the internet, the security problems he found are deeply concerning and it’s not likely that ALPR security is something that’s going to suddenly be fixed.

“Let’s say the police or Motorola were like ‘Oh crap, we shouldn’t have put those on the public internet.’ They can clean that up,” he said. “But you still have a super vulnerable device that if you gain access to their network you can see the data. When you deploy the technology into the field, attacks always get easier, they don’t get harder.”

About the author

Jason is a cofounder of 404 Media. He was previously the editor-in-chief of Motherboard. He loves the Freedom of Information Act and surfing.