Medium

Published in Beam Connectivity. 6th Febr 2025 Click to view

# Driving Cybersecurity Forward: How CHERI is transforming automotive cyber-resilience

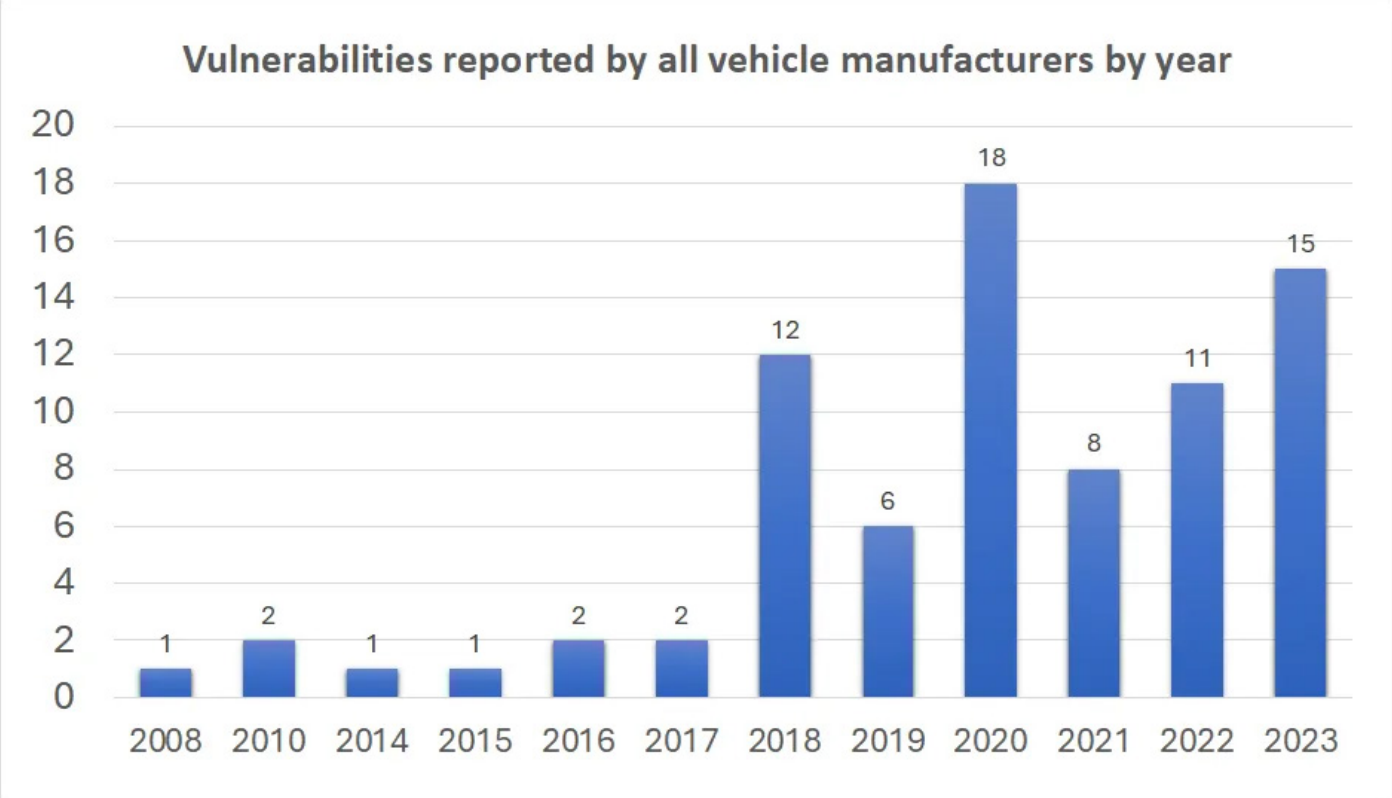
In the world of connected vehicles, cybersecurity stakes are high. Examples of hackers taking remote control of a moving vehicle have become infamous, and the costs of recalls globally related to cybersecurity vulnerabilities are estimated to run into billions of dollars.

The automotive industry's focus today is on the assurance procedures mandated by regulations such as UNECE R155, and the capabilities required to meet the ISO/SAE 21434 standard. **At Beam Connectivity, we believe a step-change in approach to the development and implementation of vehicles' cybersecurity controls is required.** This is the only way we can ensure network connections, software stacks and embedded systems are robust and resilient against malicious attackers today and in the future.

As part of our AutoCHERI R&D project, we worked with HORIBA MIRA and our project partners to demonstrate how we can achieve one such step-change.

## How many vulnerabilities are out there?

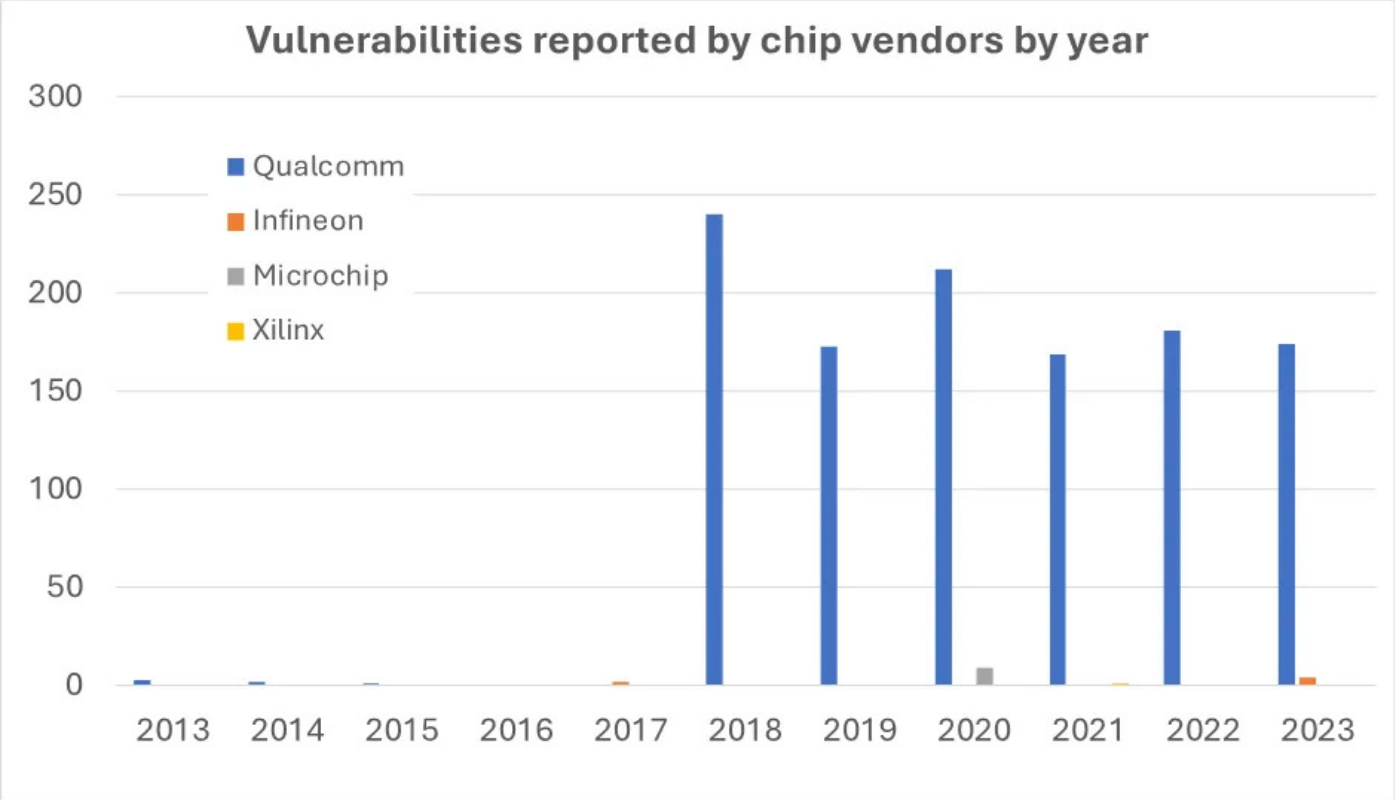
We searched through the full set of public vulnerability disclosure databases to understand just how many disclosures were being made by automotive (car) manufacturers. This is what we found.



Out of a total of 79 unique disclosures, over 60% were made by just four manufacturers: Tesla, Mercedes, BMW and Hyundai, with activity picking up noticeably in 2018. Tesla launched their "bug bounty" program for their vehicles in 2016, which coincided with the year of their first disclosure.

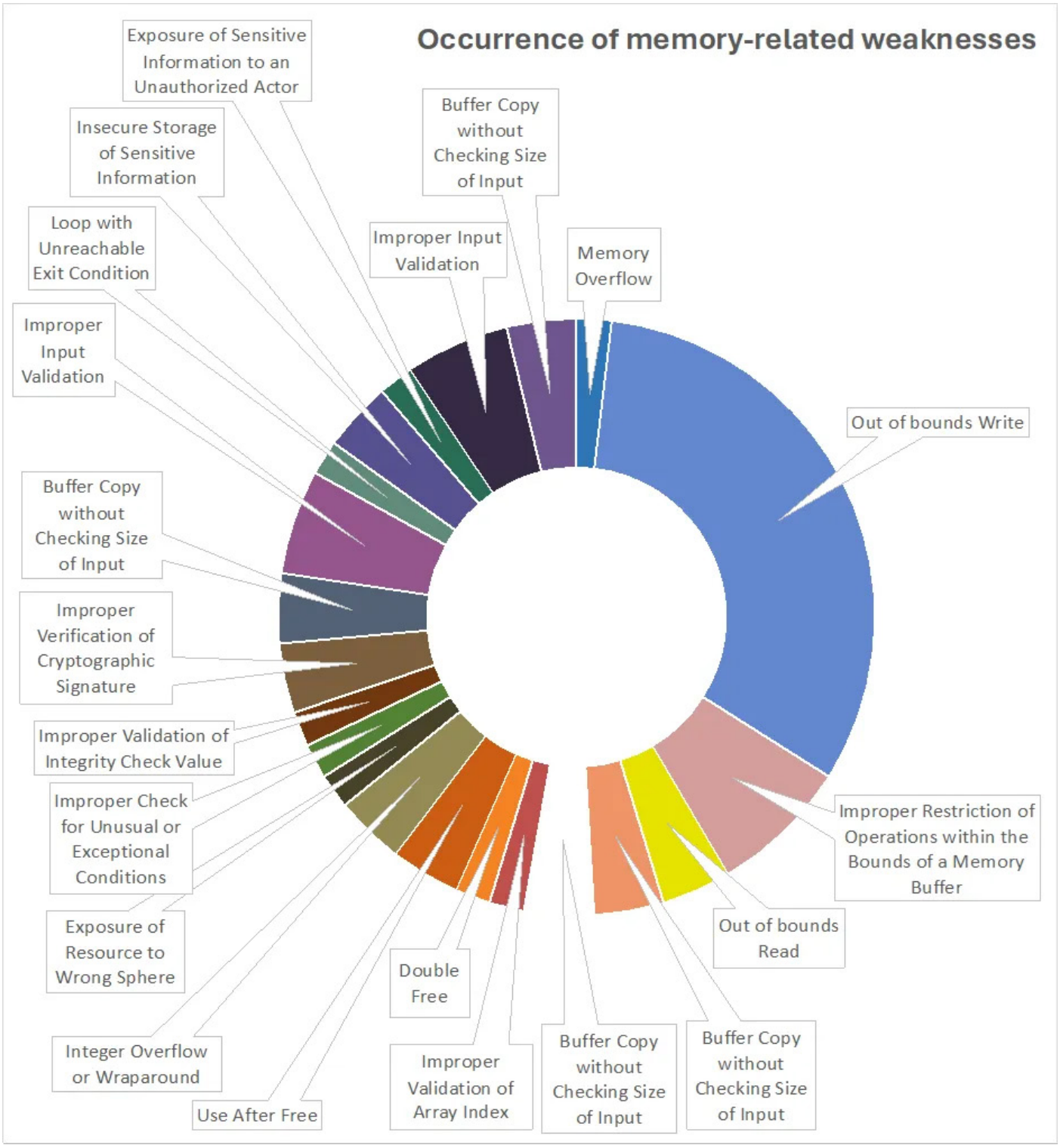
Prior to the introduction of the UNECE R155 regulation, automotive manufacturers were under no obligation to disclose vulnerabilities in any jurisdiction. The first draft of the legislation was published in December 2018, and it came into full force in July 2024.

When we looked into automotive-related disclosures made by key chip vendors, we discovered that starting in 2018 there was one company making 99% of them: Qualcomm.



## Memory safety: a critical fix

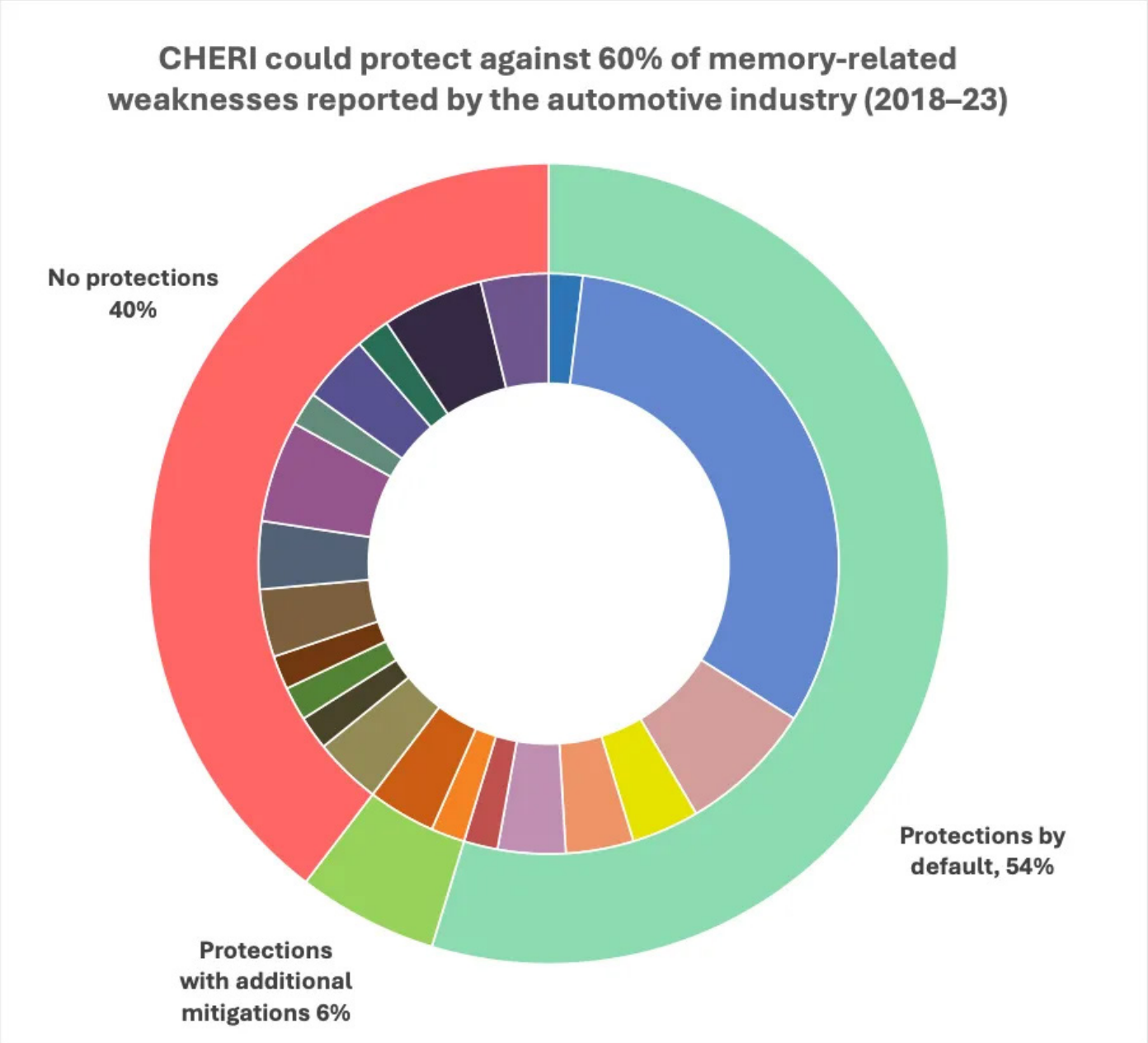
Armed with all these disclosures, we used the Common Weakness Enumeration (CWE) framework to classify all the vulnerabilities into their different types. As the goal of AutoCHERI was to address vulnerabilities related to memory safety, we then focused in on CWEs arising from improper memory usage. Here's what we found.




Of the 53 vulnerabilities related to memory usage, nearly one third were out-of-bounds writes!

## Using CHERI to address the memory safety problem

As a final step in the study, we analysed which weaknesses would be protected against by the memory safety provided by the Capability Hardware Enhanced RISC Instructions (CHERI ) technology. Here's what we found.




CHERI would protect against the majority of memory-related weaknesses, including the frequently observed out-of-bounds write, straight out of the box. With the implementation of additional mitigations, the total number of weaknesses prevented could hit 60%.

## CHERI is a critical technology to enable automotive cyber-resilience

Our study demonstrated the potential of CHERI to address memory-related weaknesses, one of the most critical sources of discovered vulnerabilities and exploits in software systems. In our next post, we will detail how we assessed the CHERI technology by building a proof-of-concept automotive connectivity system based on the Arm® Morello platform.