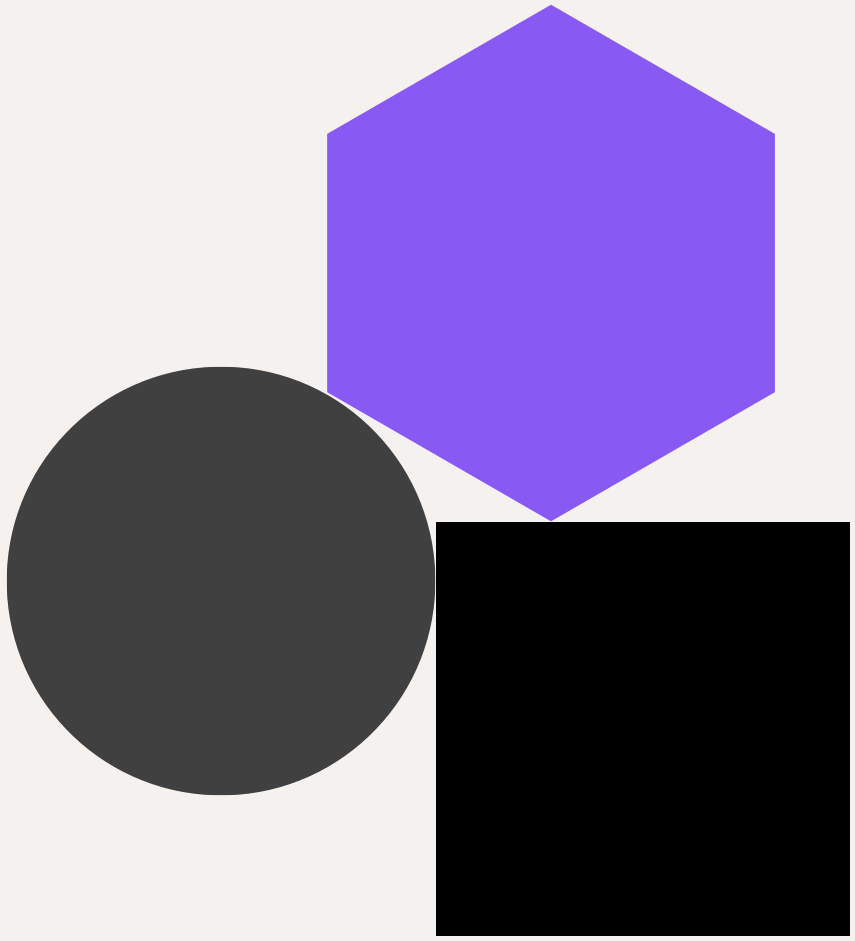
A new analysis of CVE vulnerabilites: trends, changes and CHERI

Codasip



Dr Carl Shaw

CHERI Blossoms, March 2026

Codasip

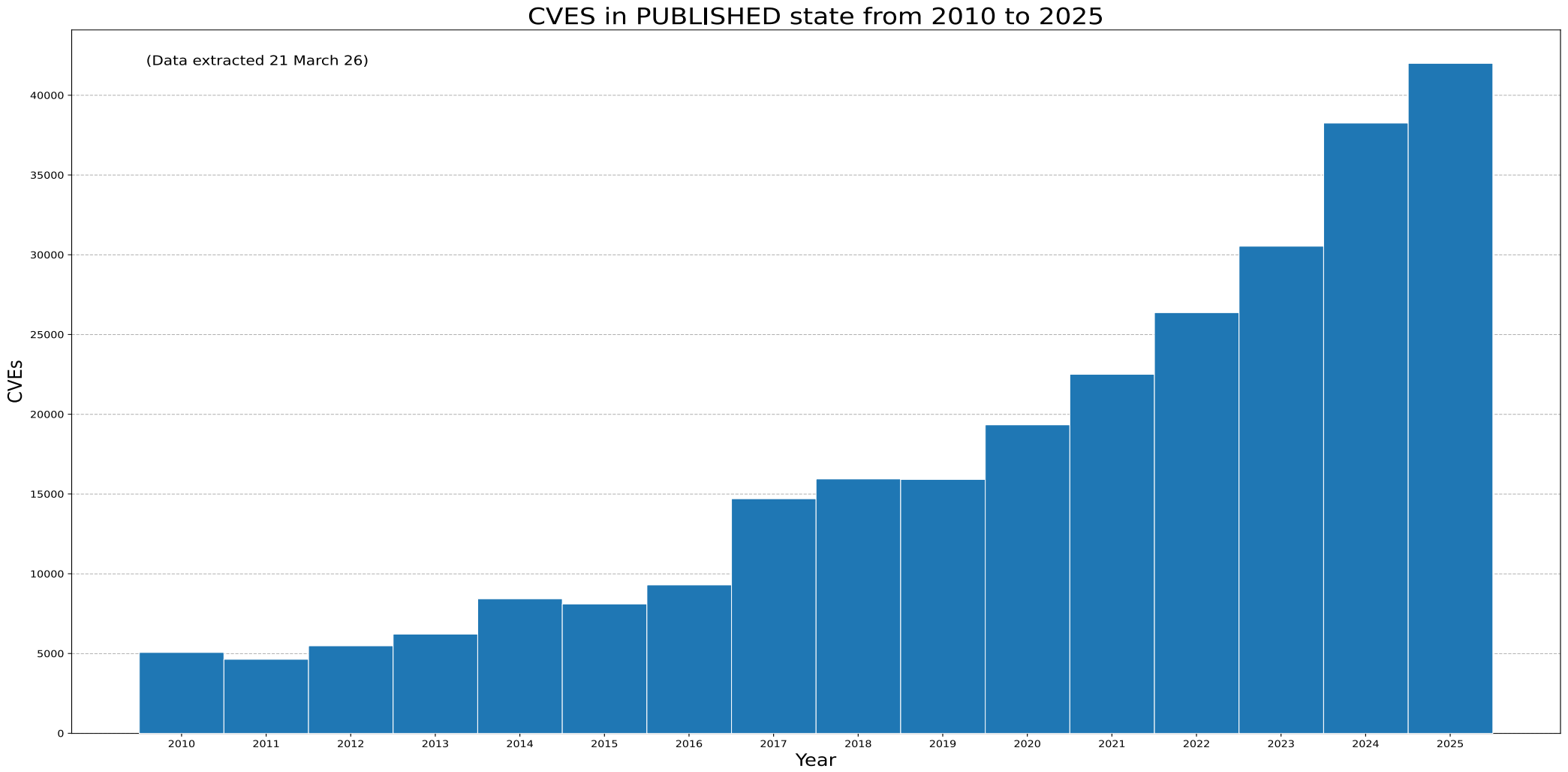
CVE:

Common **V**ulnerabilities and **E**xposures

"Identify, define and catalog publicly disclosed cybersecurity vulnerabilities"

https://www.cve.org

→ Over 314000 published CVEs and counting...



→ Why do we want to look at CVEs?

Codasip

- We need to ensure what we are doing is **relevant**
- We need to ensure we are **focusing on the right things**
- We want to **spot attack trends**

→ Why do we want to look at CVEs?

Codasip

- The CVE database should be useful:
  - Large database of vulnerabilites beginning in1999
  - Many are categorised into the type of vulnerability
  - CVEs are JSON files in a git repo (https://github.com/CVEProject/cvelistV5)
    - Machine readable
    - Contains lots of information on each vulnerability

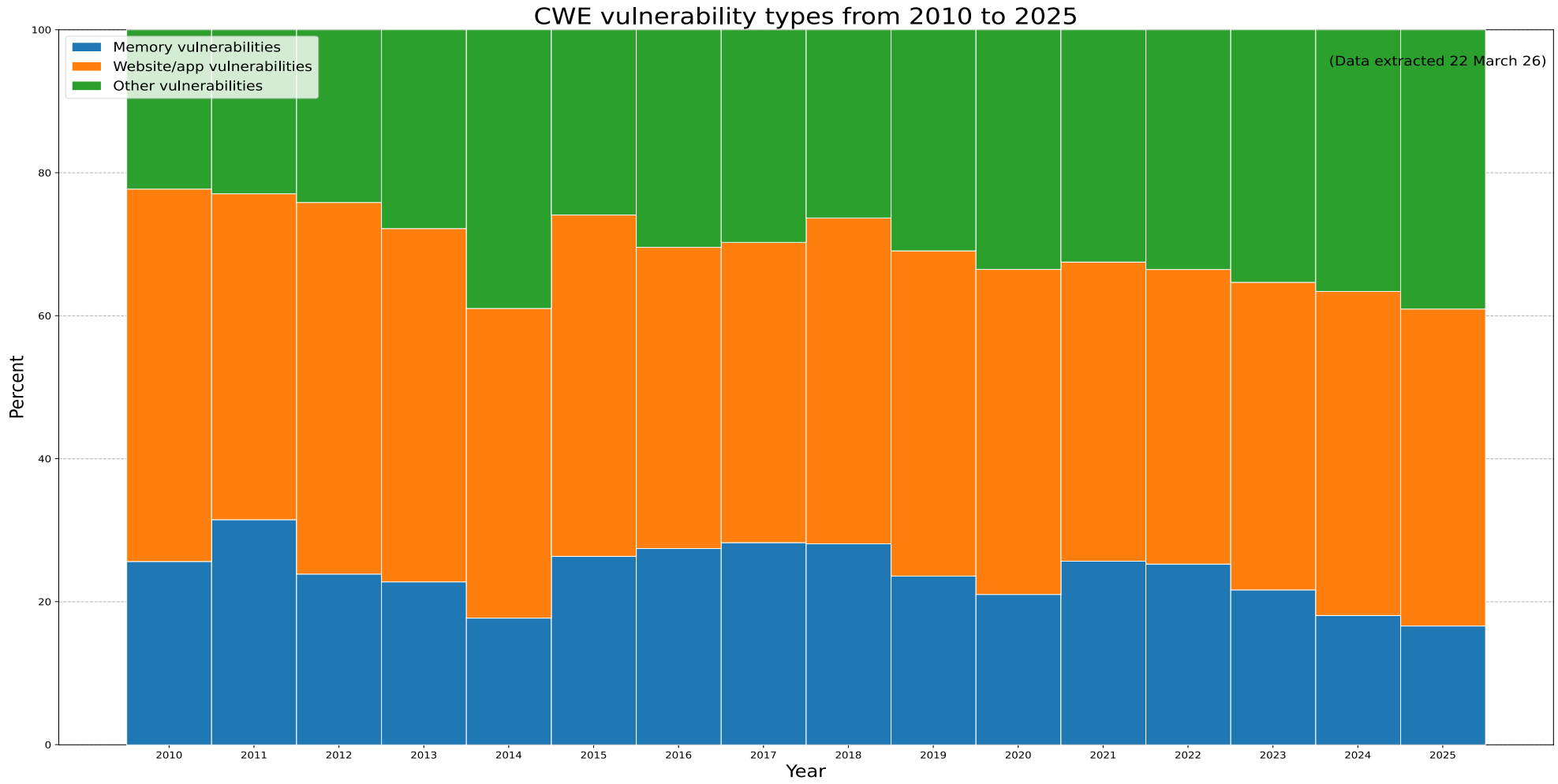
→ Classifying CVEs by CWEs

Codasip

- Many CVEs specify a CWE : the type of vulnerability
- All CVEs have a description
- We put an LLM to the task of predicting CWEs for those that didn't have one
- Good success when description was clear
- The occasional hallucination (CWE 27001?)

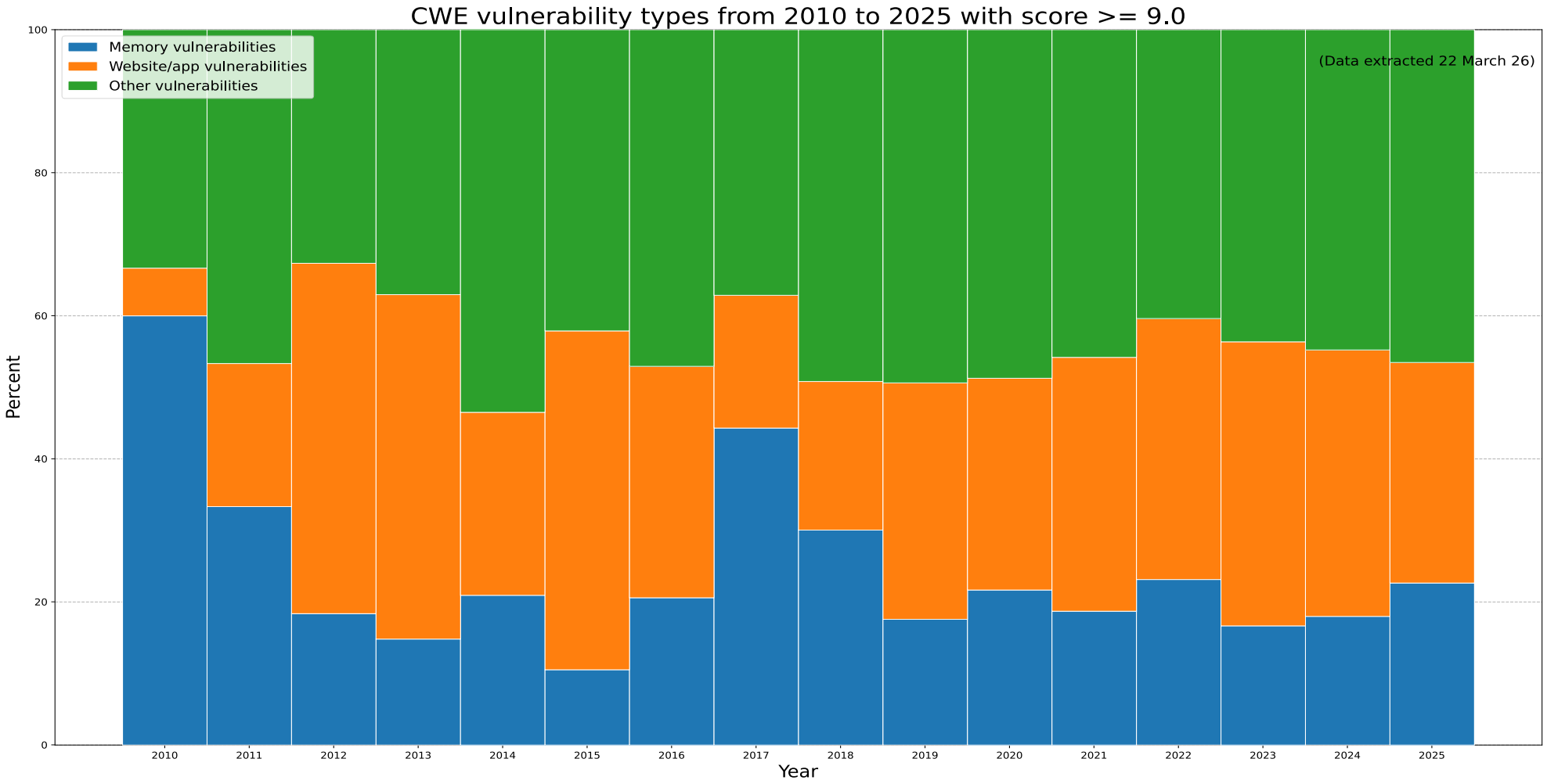
→ Classifying CVEs by CWEs

Codasip



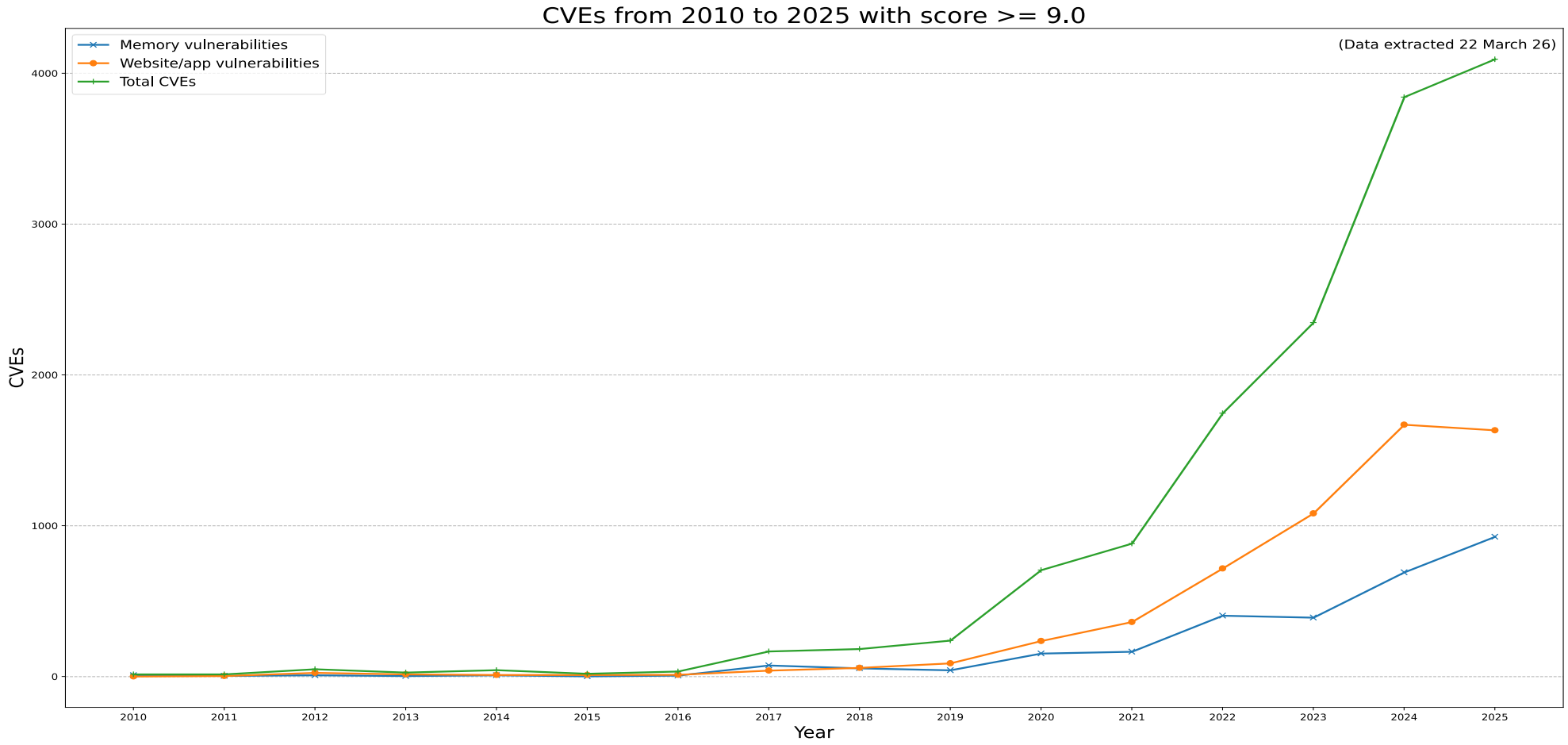
→ Classifying CVEs by CWEs

Codasip



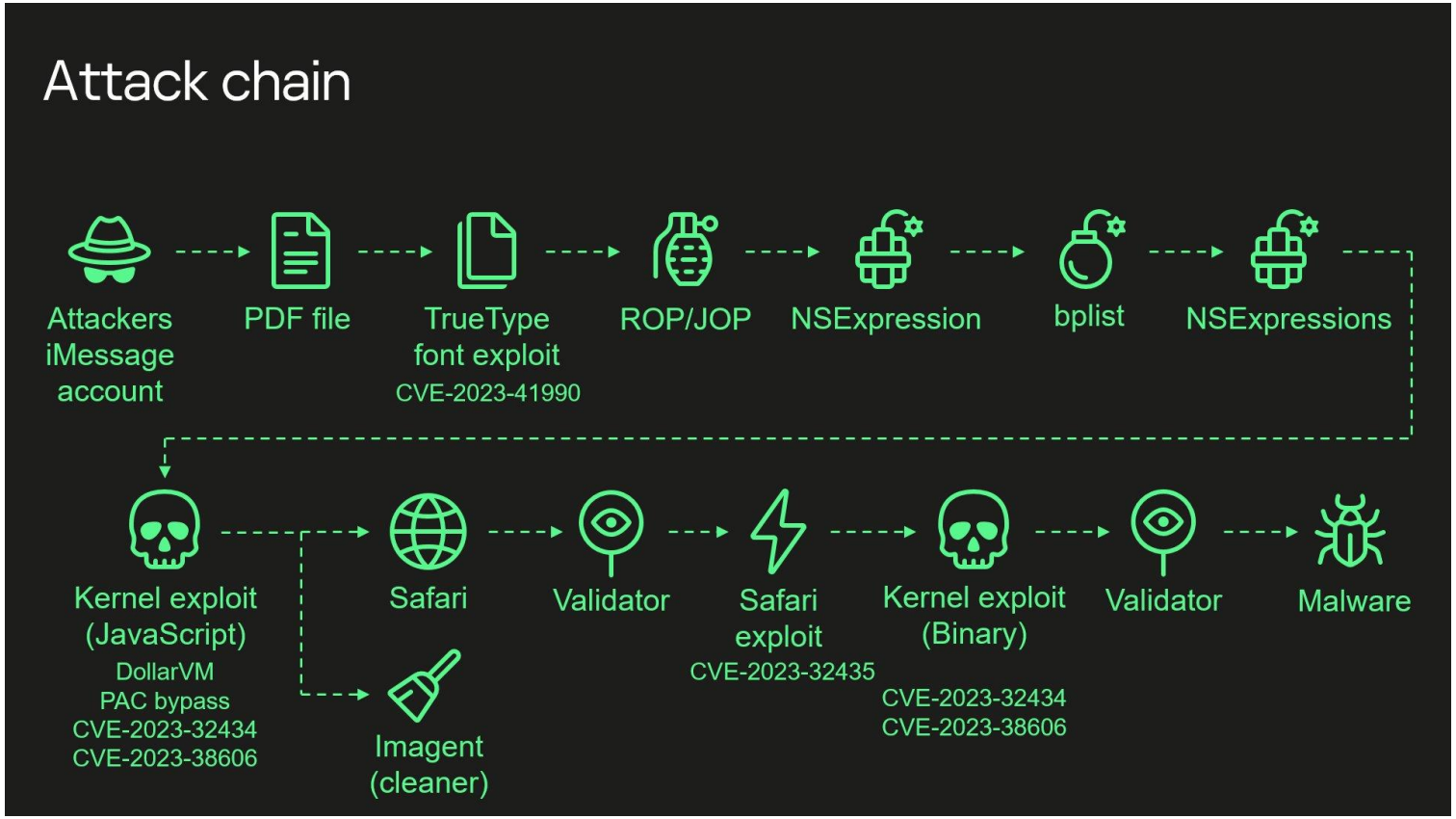
→ Classifying CVEs by CWEs

Codasip



→ Modern attacks are chains

Codasip

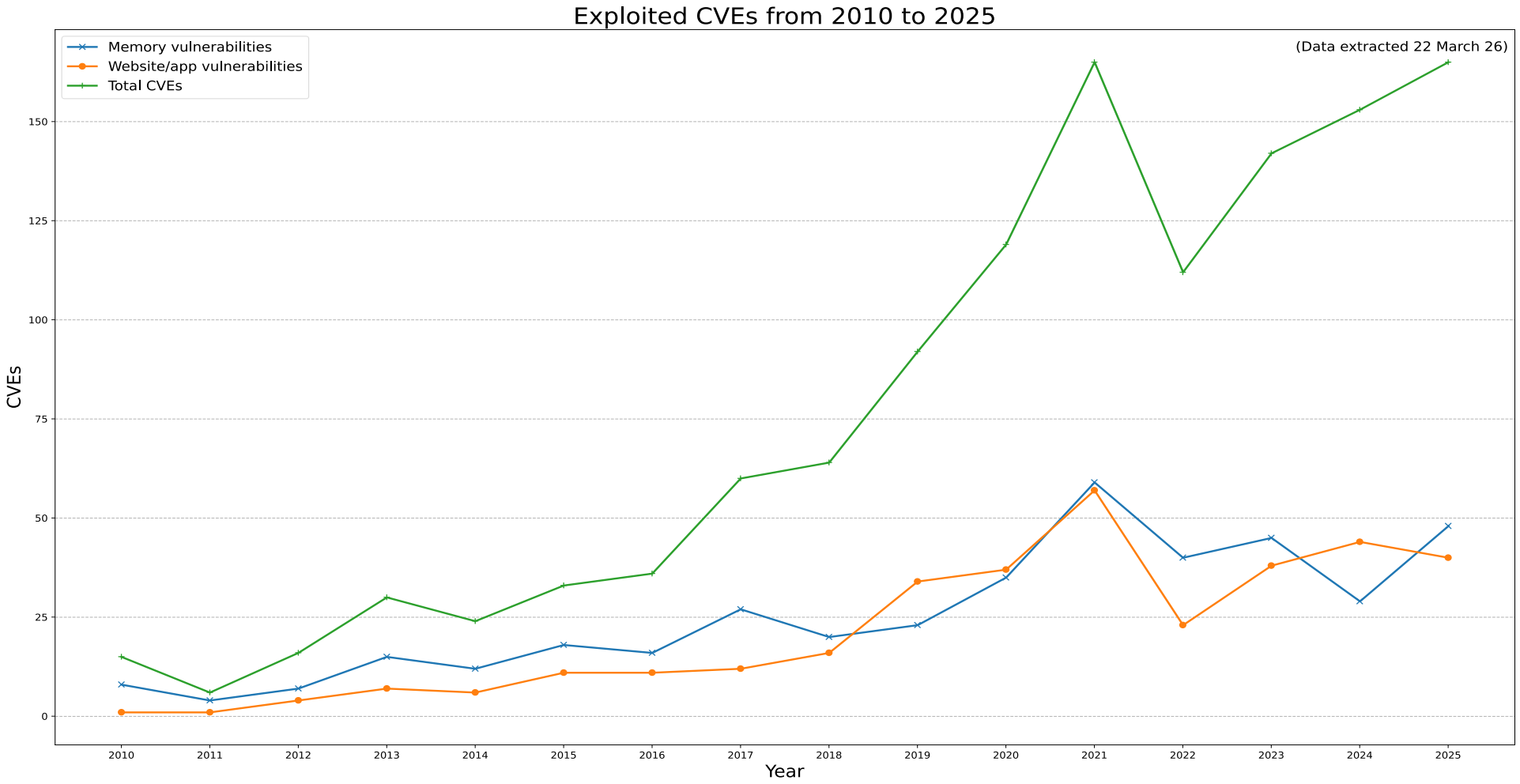


(Attack chain from Kaspersky's attack analysis of the Pegasus iOS attack https://securelist.com/operation-triangulation-the-last-hardware-mystery/111669/)

CHERI would have stopped this at the 1st exploit (CVE-2023-41990)

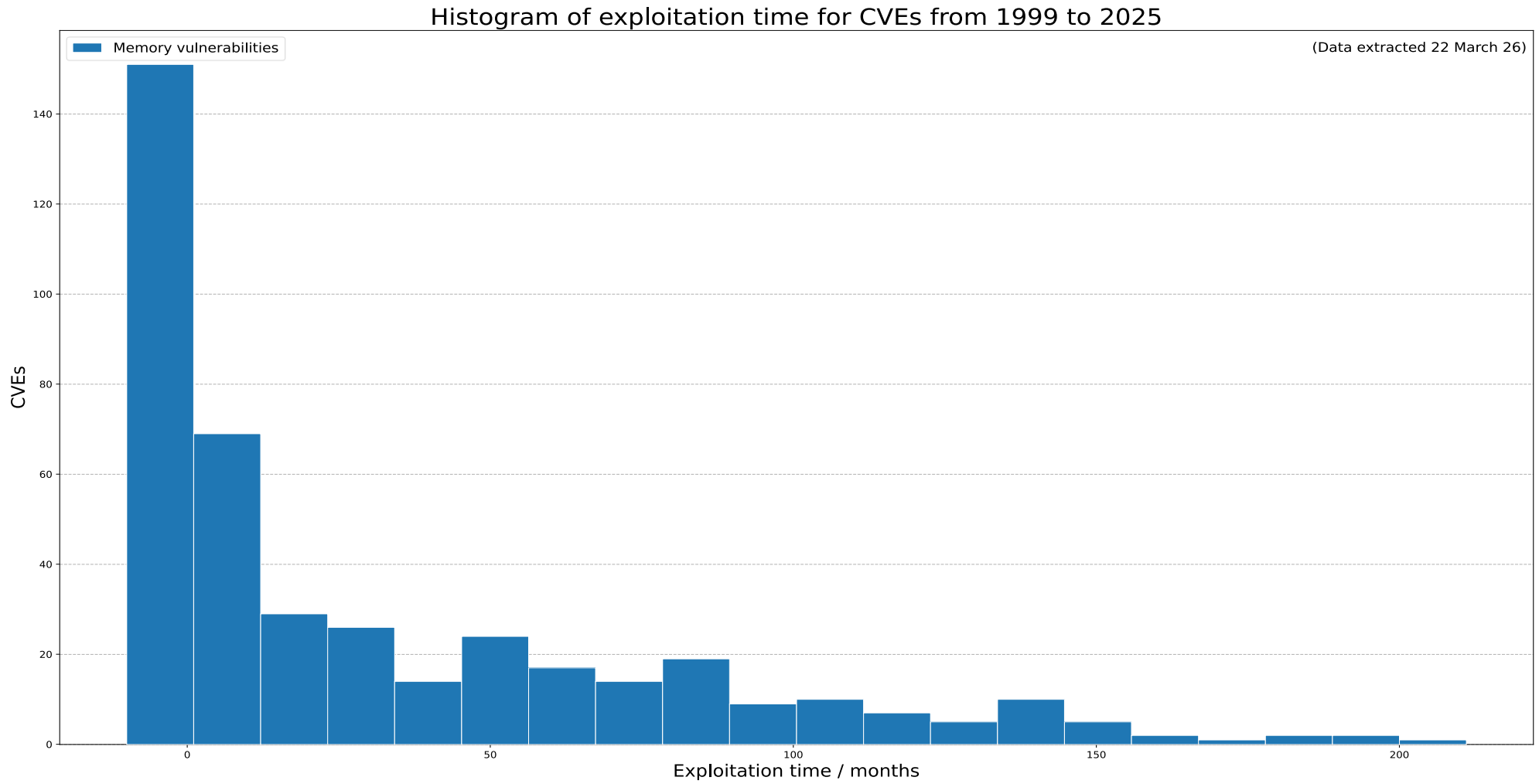
→ The Known Exploited Vulnerabilities (KEV) catalog

Codasip



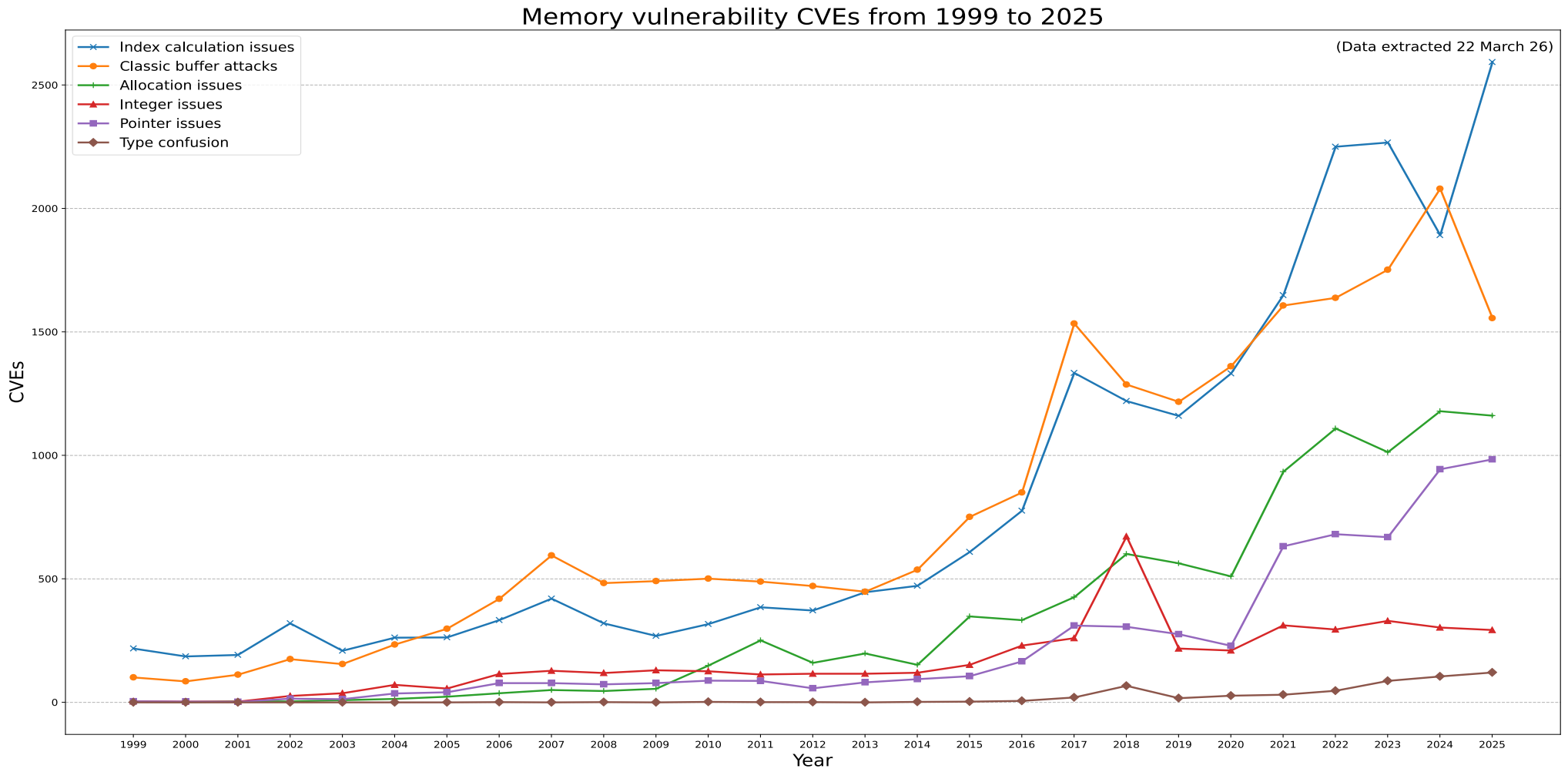
→ Time between CVE becoming public and exploitation

Codasip



→ Memory vulnerability trends?

Codasip



→ Why do we want to look at CVEs?

Codasip

- We need to ensure what we are doing is **relevant**
  - **YES – we are addressing a growing threat**
- We need to ensure we are **focusing on the right things**
  - **YES – we need a robust, long-term solution**
- We want to **spot attack trends**
  - **YES – we need to improve temporal safety**

Thank you!

carl.shaw@codasip.com