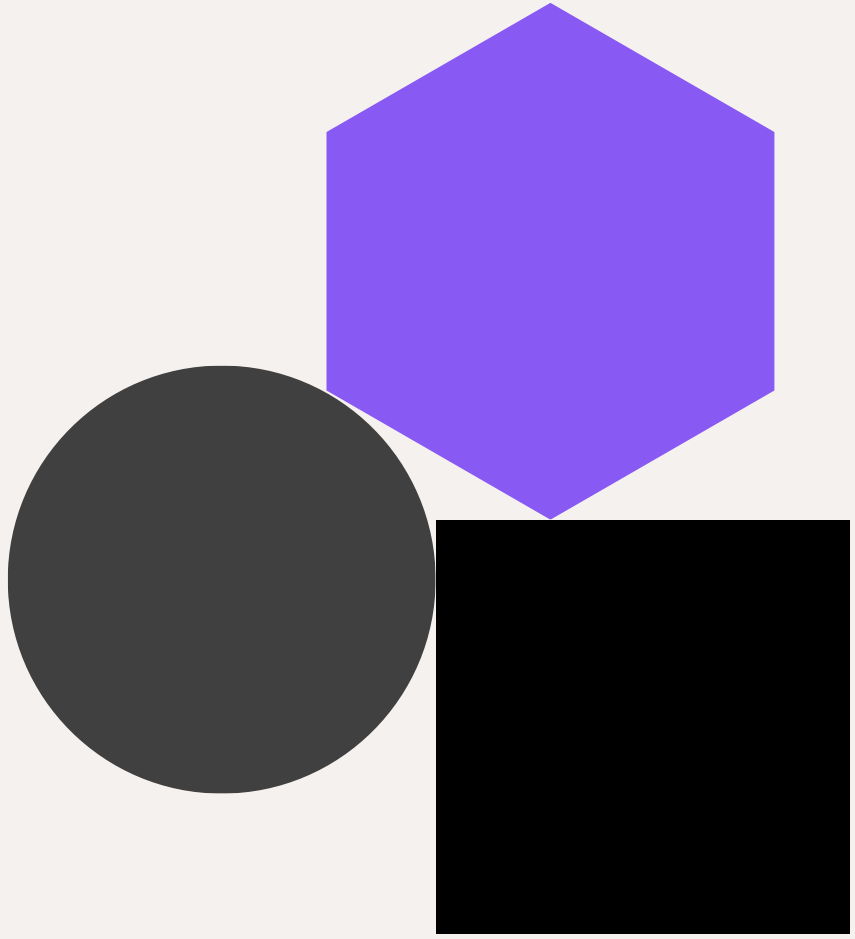
CHERI & CRA Compliance

Codasip



Why the industry needs CHERI to be able to meet the EU Cyber Resilience Act

Tariq Kurd, Codasip, UK

RISC-V Summit Europe, June 2026

→ Open source software has a lot of vulnerabilities but is widely used, for example, Linux

Codasip

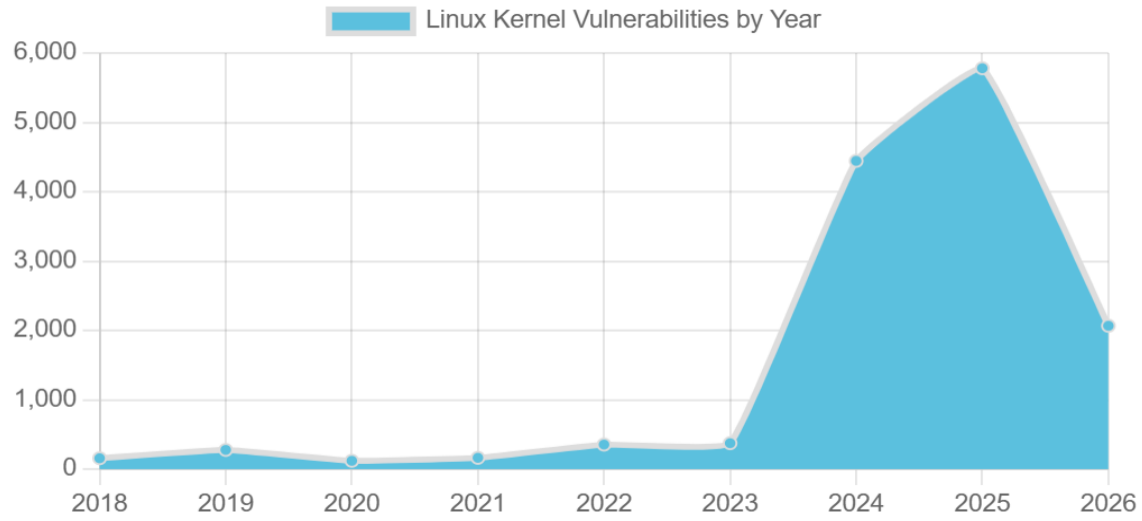
- Many consumer devices run Linux:
  - Smartphones and tablets
  - Smart TVs and Streaming Devices
  - Home Networking Gear: Most home routers, modems, and network-attached storage (NAS) devices
  - eReaders
  - Smart Home Appliances
  - Gaming Consoles
  - Etc etc.
- Open source projects are not liable under the CRA
- But products based on them are!
- 5781 vulnerabilities recorded in 2025
- Of which 4445 were in the kernel
- Manufacturers must publish fixes for nearly 16 bugs a day, across all of their devices
  - The sheer size of the maintenance required is enormous

→ Linux kernel vulnerability exploits increasing in severity

Codasip

By the Year

In 2026 there have been 2067 vulnerabilities in Linux Kernel with an average score of 8.1 out of ten. Last year, in 2025 Linux Kernel had 5781 security vulnerabilities published. Right now, Linux Kernel is on track to have less security vulnerabilities in 2026 than it did last year. However, the average CVE base score of the vulnerabilities in 2026 is greater by 2.07.



Year	Vulnerabilities	Average Score
2026	2067	8.08
2025	5781	6.01
2024	4445	6.16
2023	374	6.66
2022	354	6.44
2021	163	6.49
2020	120	6.26

Google Modem OOB Write Enables RCE

CVE-2026-0120 9.8 - Critical - March 10, 2026

In modem, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

Memory Corruption

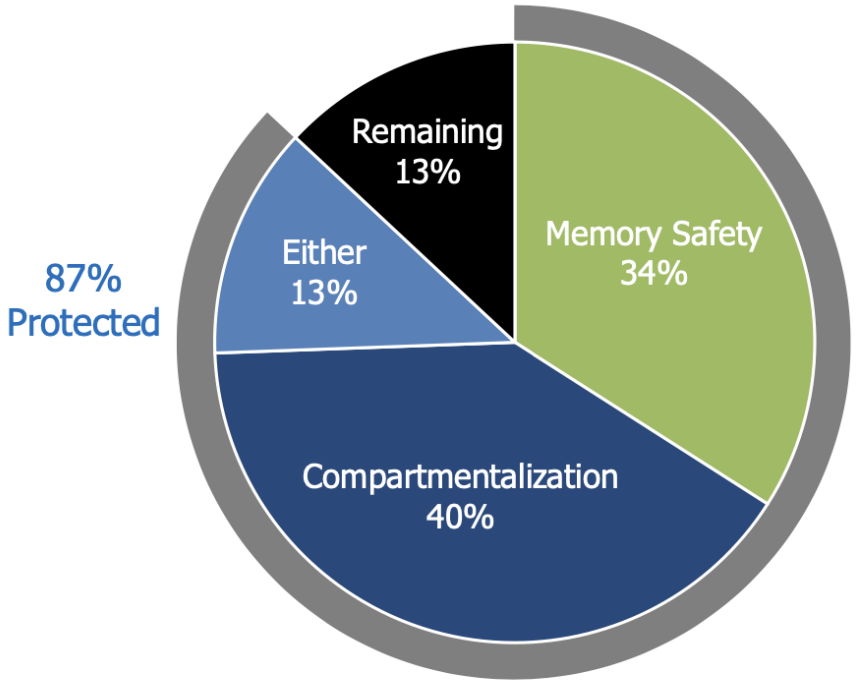
Source: https://stack.watch/product/linux/linux-kernel/

→ DARPA funded research into memory safety

Codasip

Memory safety and compartmentalization would stop most campaigns

Mitigation analysis of Linux kernel high severity CVEs



87% Protected

- Either: if memory safety or compartmentalization were present, the bug would not be exploitable
- Remaining: memory safety or compartmentalization would not mitigate the CVE

CVE: Common Vulnerabilities and Exposures

McKee, Derrick, et al. "Preventing kernel hacks with HAKC." Proceedings 2022 Network and Distributed System Security Symposium. NDSS. Vol. 22. 2022.

Distribution Statement A: Approved for public release. Distribution is unlimited.

5

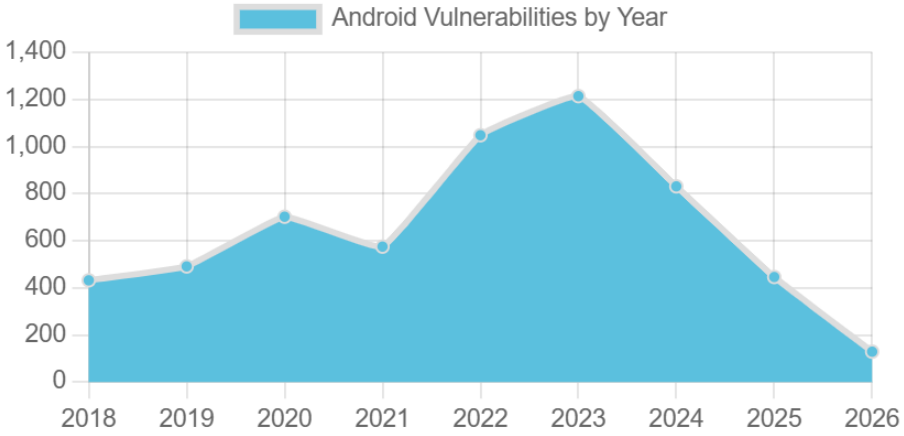
→ There are plenty of Android vulnerabilities being found

Codasip

- The total count is reduced but severity is increasing and critical exploits are real:

> Two Android vulnerabilities are now "under limited, targeted exploitation," with users at risk from "remote denial of service with no additional execution privileges needed." This is serious, as evidenced by the speed Google, Samsung and CISA have acted.
>
> CVE-2025-48633 and CVE-2025-48572 are not the only vulnerabilities flagged for December, in what has turned out to be a bumper update. But these are the highlights. Both affect Android's core framework, which runs at the core of the OS.

- Source: https://www.forbes.com/sites/zakdoffman/2025/12/04/google-issues-critical-update-for-all-pixel-users-attacks-confirmed/
- Google releases monthly patches: https://source.android.com/docs/security/bulletin



Year	Vulnerabilities	Average Score
2026	129	7.55
2025	446	7.24
2024	831	7.11
2023	1214	6.45
2022	1048	6.41
2021	575	6.72
2020	702	6.85

Source: https://stack.watch/product/google/android/

→ There were at least 8 9.8+ vulnerabilities in Android reported in March, all avoided by use of CHERI

Codasip

Android DeviceId.java Bounds Check Vulnerability: Local PrivEsc via Desync

CVE-2025-48611 10 - Critical - March 10, 2026

In DeviceId of DeviceId.java, there is a possible desync in persistence due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

Classic Buffer Overflow

Google Modem OOB Write Enables RCE

CVE-2026-0120 9.8 - Critical - March 10, 2026

In modem, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

Memory Corruption

OUT-OF-BOUNDS WRITE IN mfc_core_isr.c OF Google Nest, RCE

CVE-2026-0116 9.8 - Critical - March 10, 2026

In __mfc_handle_released_buf of mfc_core_isr.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.

Memory Corruption

CVE-2026-0110, 0111, 0112, 0113, 0114 are all very similar to 0116 - Source: https://stack.watch/product/google/android/

→ Cyber security has never been so high profile

Director GCHQ warns UK at ‘moment of consequence’ in inaugural Annual lecture

Today (Wednesday 27 May 2026) Director GCHQ Anne Keast-Butler delivered the first Annual Lecture at Bletchley Park

Taking to the stage at the Fellowship Auditorium at GCHQ’s wartime home of Bletchley Park, Director GCHQ Anne Keast-Butler emphasised the importance of international partnerships for increasing resilience and harnessing technology for good amidst a *“narrowing window for the UK and allies to stay ahead.”*

Marking the 80th anniversary of the UKUSA intelligence agreement, Director GCHQ set out the nature of the threat as seen by the organisation and detailed how partnerships – from AI to intelligence, and academia to the public – are the crux of our resilience and prosperity in the face of such challenges. She continued to urge us all to take action, *“from living rooms to boardrooms”* *to make cyber security “ten times more urgent.”*

Source: https://lnkd.in/ezzdhvPz

→ Cyber security regulation is approaching fast…

Codasip

EU Cyber Resilience Act (CRA)
sets mandatory security obligations for **ALL*** products with **DIGITAL ELEMENTS** **sold into the EU**
(fully applicable Dec 2027)

It requires manufacturers to secure their products

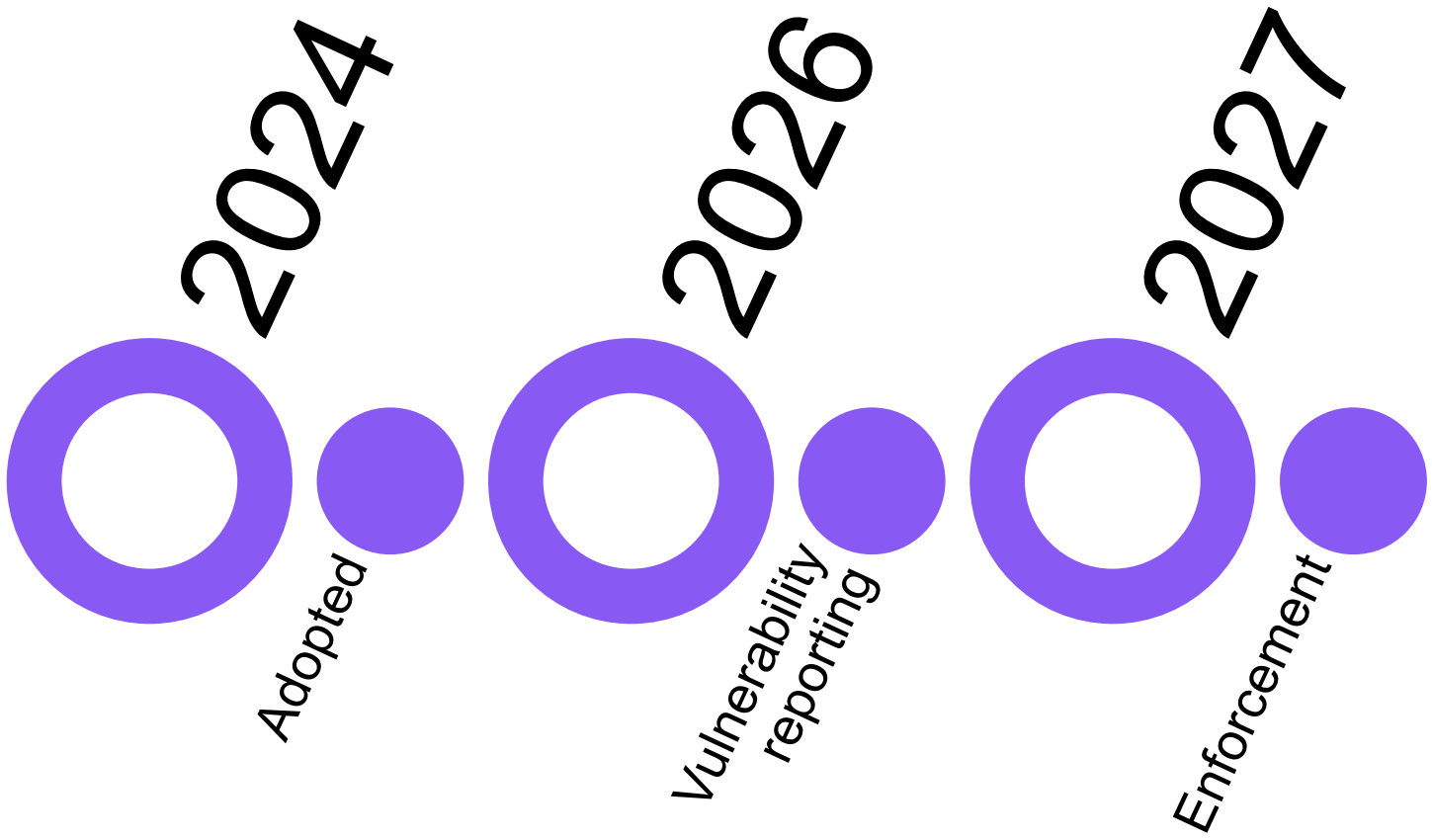
→ CRA Core requirements (Annex I):

- Secure by design & security enabled by default
- Protection against known **exploitable vulnerabilities**
- Attack surface minimization
- Reduction of incident impact
- Lifecycle vulnerability management

→ CRA Vulnerability reporting obligations (Art. 14):

- After “a severe incident having an impact on the security of the product”
  - “early warning notification” within 24 hours
  - “provide general information” within 72 hours
  - “applied and ongoing mitigation measures” with one month

→ CRA Deadlines



- Sept 11, 2026: Incident reporting obligations begin (Art. 71 (2) / Art. (14))
- Dec 11, 2027: Full compliance required for market access (Art. 71 (2))

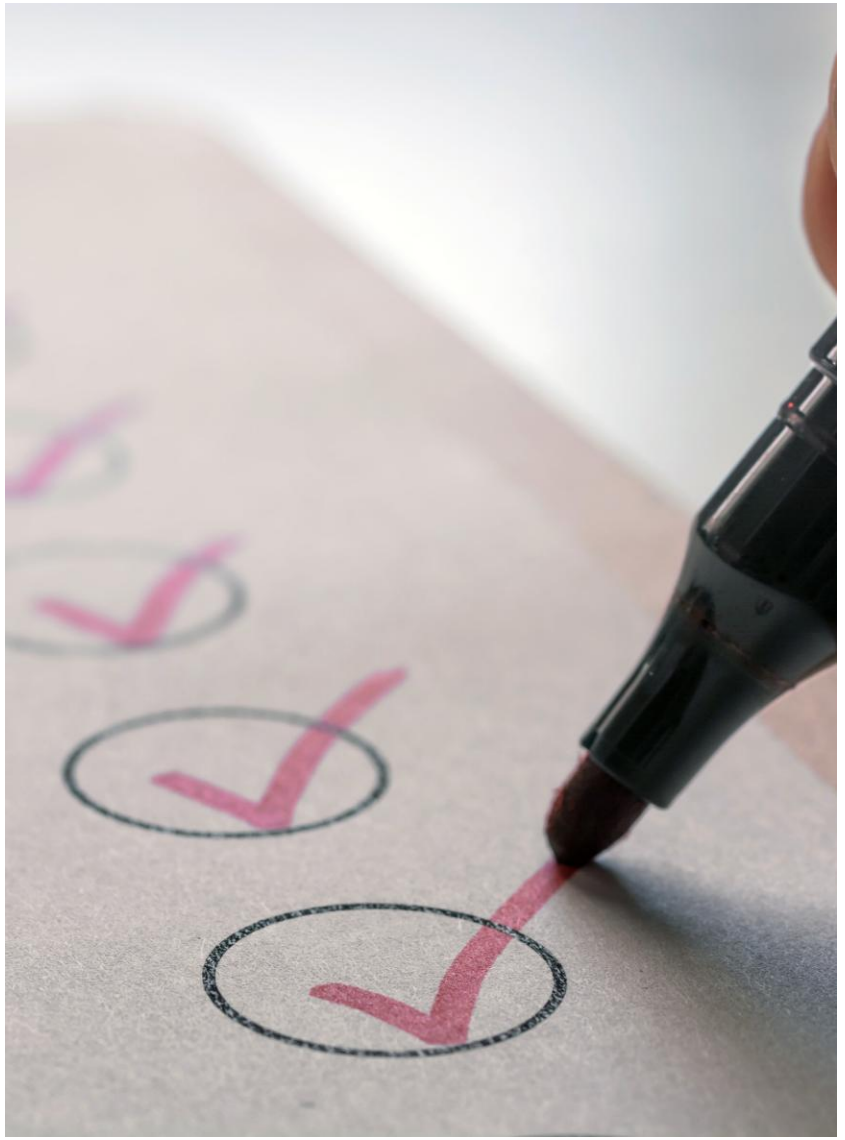
→ CRA is Regulation with Consequences

Codasip

- Maximum fine: **€15 million or 2.5% of global annual turnover**, whichever is higher.
  - These penalties apply to serious violations such as:
    - Placing non-compliant products on the EU market.
    - Failing to address known exploitable vulnerabilities.
    - Ignoring mandatory security update obligations.
- National authorities can **prohibit or restrict product sales** in the EU if a product:
  - Poses a cybersecurity risk.
  - Lacks required CE marking or documentation.
  - Fails to meet CRA's essential requirements.
- Authorities may **order product recalls** or **force withdrawal from the market**
  - Article 20 (4)

→ **Manufacturer obligations** (Arts. 6–10):

- Risk assessment of products
- Secure by design
- Vulnerability handling & reporting (24hrs!)
- Supply chain security
- Documentation & CE marking
  - CRA compliance will be required for CE
- Minimum 5 year support & updates
  - Or longer if the expected lifetime is longer



→ Addressing CRA requirements with CHERI

Codasip

CRA Requirement	CHERI Contribution
Secure by design, No known exploitable vulnerabilities	Software defined and hardware-enforced memory safety
Lifecycle Security	Greatly reduced risk of finding new exploits requiring software updates
Limited Attack Surface	Attack surface is limited by design
Impact Reduction	Incident impact reduced by memory safety and software isolation (compartmentalization)
Disclosures and updates	Greatly reduced risk of finding new exploits requiring disclosures
Third-party and open-source software	Compartmentalization greatly restricts the potential harm from third party and open-source software

→ Benefits of CHERI for Manufacturers

Codasip

- Lower lifecycle costs - fewer vulnerabilities to manage
- Faster CRA conformity assessments
  - Clear evidence of secure design
- Competitive advantage in the EU market
  - *“CRA-ready hardware security”*
- Reduced risk of brand damage
  - Vulnerabilities **must** be publicly disclosed from September 2026
- Reduced liability, regulatory and product recall risk
- Significantly safer devices for consumers with dramatically reduced risk of zero click exploits

→ Conclusion

Codasip

- CRA requires **secure by design** products
- CHERI provides a **hardware foundation** for compliance
- Adoption **now** prepares manufacturers for 2026–2027 deadlines
  - Silicon manufacturers must act immediately for product manufacturers to be ready

CHERI = compliance + resilience + market advantage