CHERITech'26

Why a Cyber Security Agency Cares About CHERI



Federal Office
for Information Security

Credits: © AdobeStock/Nirut

The Importance of Memory Safety

Attacker compromised nearly 1000 Zyxel switches since August (CVE-2026-7273)

A Chinese-speaking threat actor has exploited a vulnerability (CVE-2026-7273) in unpatched ZyXEL GS1900 Smart Managed Switches and has exfiltrated sensitive data from 996 devices across 48 countries, GreyNoise reported on Monday.

- We all know about memory safety vulnerabilities
- Reliance on existing, memory unsafe code basis (e.g. C/C++)
- LLMs as accelerators of cyber (in)security
  - increase in reported vulnerabilities
  - faster code generation
  - time between appearance of a vulnerability finding and exploitation decreases
- Regulations recognize cyber-weakness

Memory Safety

What is being done?

- Adoption of memory-safe languages progresses
- BSI recognizes importance and supports certain efforts
- Recent regulations “demand” it

The (successful) end of the kernel Rust experiment

[Posted December 10, 2025 by corbet]

https://lwn.net/Articles/1049831/

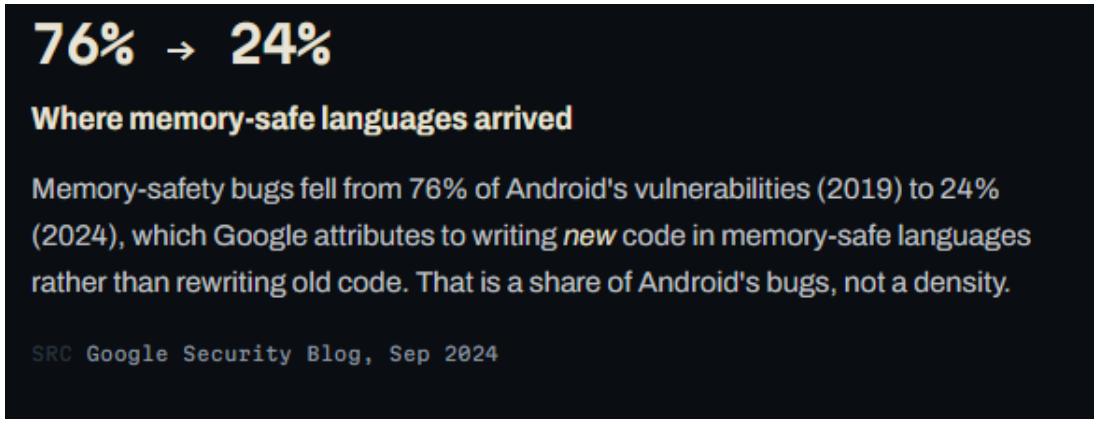


https://trifectatech.org/docs/improving-europes-cybersecurity-posture-through-memory-safety.pdf

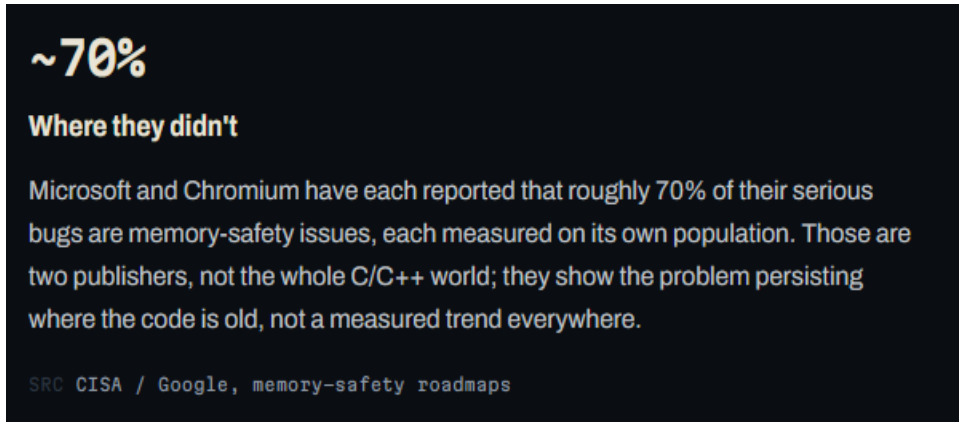
Memory Safety

Are we doing enough?

- Memory-safe programming languages help for *new* code
- Memory-safety vulnerabilities are still omnipresent
- We can’t rewrite everything



https://vulnerabilitydata.io/types



https://vulnerabilitydata.io/types

Why CHERI

From a cyber security agency‘s point of view

- Prevents whole classes of vulnerabilities
- Reduces blast radius
- Security by design
- Scalability (for old/large code bases)
- Complements other mitigations (e.g. Fuzzing in a Memory Safe Verification Environment)
- Makes compliance easier (for both sides)
- Transparency and Trustworthiness
  - Public architectural specifications with formal, executable models
  - Peer-reviewed research, openly available

In light of current regulation

- What a lot of regulation wants: good baseline security
- CHERI easily solves this for memory safety
- Fits perfectly with regulations such as CRA and NIS-2
- CRA demands a lot
  - Reporting obligations
  - Patching obligations
  - Security by design (see examples)
  - CHERI can make all of this much easier

Part I Cybersecurity requirements relating to the properties of products with digital elements

(1) Products with digital elements shall be designed, developed and produced in such a way that they ensure an appropriate level of cybersecurity based on the risks.

(2) On the basis of the cybersecurity risk assessment referred to in Article 13(2) and where applicable, products with digital elements shall:

(a) be made available on the market without known exploitable vulnerabilities;

(j) be designed, developed and produced to limit attack surfaces, including external interfaces;

(k) be designed, developed and produced to reduce the impact of an incident using appropriate exploitation mitigation mechanisms and techniques;

Existing Challenges

- Availability of (general-purpose) hardware
- Architectural standardisation
- Test coverage (“will my stuff still work”) and tooling / software ecosystem
- OS integration
- Temporal safety

Outlook

From our perspective

- Where should CHERI come first?
- A lot of use cases benefit from a quick adoption
  - large legacy code bases in memory-unsafe languages
  - hard-to-patch, long-living systems
  - safety- or availability-critical systems
- CHERI can be a more practical route to meeting security requirements compared to alternatives like large-scale rewrites
- What it takes to beat the challenges:
  - *Can I get it?* → General-purpose hardware and a stable, standardised architecture
  - *Will my stuff work?* → Test coverage, tooling and OS integration
  - *Does it protect enough?* → Temporal safety, and clear labelling of what a product really covers
- BSI will continue to support incentives to invest in memory-safe hardware

Thank you! Questions?

Yona Raekow,

Head of Division IT-Systems

Federal Office
for Information Security

Follow us:

Credits: © AdobeStock/Nirut