

31 March 2026



CHERI

CHERI: quantifying the value of a strategic imperative

Ollie Whitehouse

CTO, National Cyber Security Centre

○ Quantifying the value of a strategic imperative



We quantify
returns

We evidence we have
no better scaled
strategy to address
memory safety

We quantify the
cost of adoption and
reduce relentlessly

○ Agenda

- ◆ The Strategic Imperative
- ◆ Quantifying The Value
- ◆ Barriers
- ◆ A Future To Aim For
- ◆ Closing

The Strategic Imperative

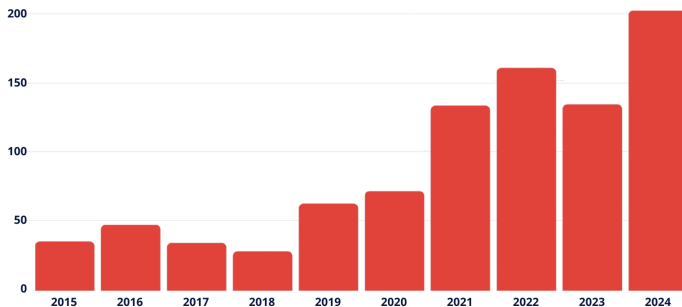
○ Strategic Imperative



Memory Safety Known Exploited Vulnerabilities

VuInCheck

● Memory Safety



May 2025 - <https://runsafesecurity.com/blog/memory-safety-keys-increasing/>

○ Strategic Imperative



Citrix NetScaler customers hit by third actively exploited zero-day vulnerability since June

The vendor, which has been widely targeted, said the memory-overflow vulnerability can result in remote-code execution or denial of service.

BY **MATT KAPKO** - AUGUST 26, 2025

🔊 Listen to this article 3:52 Learn more.

<https://cyberscoop.com/citrix-netscaler-zero-day-exploited-august-2025/>

Do Secure-By-Design Pledges Come With Stickers? - Ivanti Connect Secure RCE (CVE-2025-0282)

<https://labs.watchtower.com/do-secure-by-design-pledges-come-with-stickers-ivanti-connect-secure-rce-cve-2025-0282/>

yIKEs - IKEv2 Out-of-Bounds Write

CVE-2025-9242

Today is the **8th of November 1996**, and we're thrilled to be exploring this new primitive we call Stack-based Buffer Overflows. It's a great time to be alive, especially because we don't have to deal with any of the pain of modern/not-so-modern mitigations.

Oh no, wait, it's 2025 and we are still seeing Stack-based Buffer Overflows in enterprise-grade appliances, and of course, lacking mainstream exploit mitigations.

<https://labs.watchtower.com/yikes-watchguard-fireware-os-ikev2-out-of-bounds-write-cve-2025-9242/>

○ Strategic Imperative



A 32-Year-Old Bug Walks Into A Telnet Server (GNU inetutils Telnetd CVE-2026-32746 Pre-Auth RCE)

<https://labs.watchtower.com/a-32-year-old-bug-walks-into-a-telnet-server-gnu-inetutils-telnetd-cve-2026-32746/>

○ Strategic Imperative



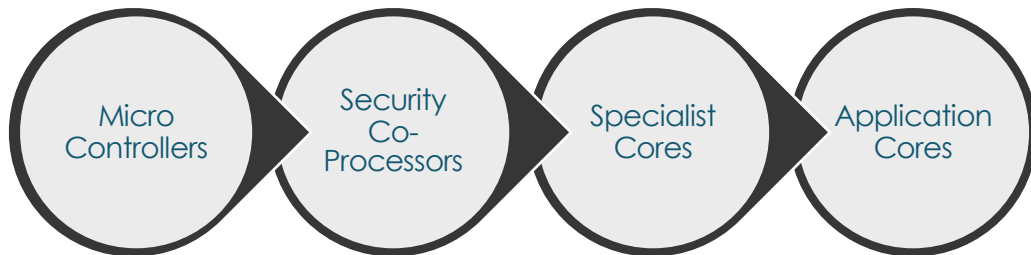


Strategic Imperative



we have time, but not limitless

○ Strategic Imperative





Quantifying The Value

Quantifying The Value - vendor



of the competitive edge

○ Quantifying The Value - vendor



of the increased velocity

○ Quantifying The Value – the vendor



of the human cost savings

○ Quantifying The Value – the vendor



of the patches that never were
(sustainment cost)

○ Quantifying The Value - vendor



of the cost saving compared to re-languaging

○ Quantifying The Value - vendor



of the technical debt management

○ Quantifying The Value - customer



of the extended life

○ Quantifying The Value – all



of the breaches that never were
(inc supply chain e.g. xz)

Quantifying The Value - all



of the impact which was reduced

○ Quantifying The Value – vendor & customer



of the reduced cost of compliance

○ Quantifying The Value – vendor & customer



of the reduced cost of liability

Barriers

Barriers



null hypothesis

○ Barriers



incentives

Barriers



transparency in technology

○ Barriers



availability

○ Barriers



bill of material cost

Barriers



test case coverage

Barriers



tooling availability and quality



A Future To Aim For

○ A Future To Air For



To prototype with
CHERI cores
is defacto

To uplift code at scale
with confidence is
efficient and easy

To not use CHERI is
unavoidable

Closing



Closing..



We quantify
returns

We evidence we have
no better scaled
strategy to address
memory safety

We quantify the
cost of adoption and
reduce relentlessly

Questions



CHERI

THANK YOU

Contact ollie.whitehouse@ncsc.gov.uk

Web www.ncsc.gov.uk