EINPRESSWIRE

# TrustInSoft Confirms Alignment with CISA Cybersecurity Initiative

*TrustInSoft Comments on Cybersecurity and Infrastructure Security Agency “Product Security Bad Practices”*

PARIS, FRANCE, December 12, 2024 /EINPresswire.com/ -- TrustInSoft, a leading provider of advanced software analysis tools, has commended an initiative by the Cybersecurity and Infrastructure Security Agency (CISA) to identify and address key security practices for enhancing the quality and safety of software products, particularly across industries such as automotive, aerospace, defense, consumer electronics, and IoT industries. TrustInSoft cited a document recently published by the U.S. Department of Homeland Security on product security bad practices (docket CISA-2024-0028), in particular areas pertaining to memory-unsafe languages like C and C++ and offered constructive comments to help inform ongoing cybersecurity developments.

> “
> While memory-related vulnerabilities indeed remain a major security concern, we would like to highlight the continued relevance of C and C++”
>
> *Benjamin Monate, Chief Technical Officer, TrustInSoft*

“While memory-related vulnerabilities indeed remain a major security concern, we would like to highlight the continued relevance of C and C++,” wrote Benjamin Monate, Chief Technical Officer, TrustInSoft. Monate elaborated, writing that, “C and C++ languages have a vast repository of well-established libraries that are extensively used across numerous industries. Many organizations rely on these libraries to deliver robust functionality, and transitioning to a new programming language would demand significant cost and effort, especially for regulated sectors requiring specific certifications and compliance.” He added that modern, next-generation sound and exhaustive static analyzers such as TrustInSoft Analyzer (TISA) support CISA's software security efforts by offering tools that mathematically prove the absence of memory-related vulnerabilities in software written in C and C++.

These tools are capable of scaling large codebases and offer comprehensive detection of undefined behaviors, including memory safety vulnerabilities. Such analyzers have matured to a level where they can be incorporated at various stages of the software development lifecycle (SDLC) and can be invaluable for the vast number of organizations that rely on C and C++. TISA differs from other tools on the market due to its ability to provide mathematical guarantees of software safety, which goes beyond the heuristic-based detection offered by traditional static or dynamic analyzers. Recognized by the U.S. National Institute of Standards and Technology (NIST) for leveraging advanced formal methods, including abstract interpretation, TrustInSoft can mathematically guarantee analyzed software is free of critical runtime errors and vulnerabilities.

Benjamin Monate, Chief Technical Officer, TrustInSoft

TrustInSoft Logo

In his comments, Monate went on to acknowledge that while memory-safe languages like Rust offer promising alternatives, their toolchains do not yet fully support the full range of embedded microcontrollers used across critical industries. For many organizations, C and C++ remain the most viable options, given the available and reliable toolchains compatible with diverse hardware platforms. It was also suggested that the CISA provide further clarity around the definition of “product” scope, as outlined by the European Union in the Cyber Resilience Act ([https://www.european-cyber-resilience-act.com/](https://www.european-cyber-resilience-act.com/)), which would help organizations to ensure adherence with CISA guidelines. In view of these considerations, Monate recommended additions to the CISA that could be included in the final CISA document. [https://www.regulations.gov/document/CISA-2024-0028-0001](https://www.regulations.gov/document/CISA-2024-0028-0001)

Monate said, “When using memory-unsafe languages (e.g., C/C++) or unsafe features of a memory-safe language, it is advisable to employ sound and exhaustive static analyzers that use formal verification techniques. These tools can ensure thorough coverage and identify memory-related bugs, enhancing the security of codebases. “A dedicated security activity should be embedded within the SDLC, leveraging state-of-the-art tools (sound static analyzer) and processes during development, testing, and maintenance phases. This aligns with the Shift Left paradigm, which advocates for early integration of security measures. “Continuous Integration/Continuous Deployment (CI/CD) pipelines should incorporate security checks as part of automated workflows, ensuring regular and consistent assessments. “And for high-criticality products or sensitive libraries - based on threat models - organizations should conduct thirdparty security assessments before product release. Depending on product criticality, such assessments could range from detailed bug reporting by sound and exhaustive static analyzers to physical testing, e.g., penetration testing and security certifications by accredited security labs."

Software developers and cybersecurity professionals can explore the benefits of TrustInSoft Analyzer by visiting TrustInSoft's website or by scheduling a demo - [https://www.trust-in-soft.com/book-a-demo](https://www.trust-in-soft.com/book-a-demo). They can also contact TrustInSoft to discuss details about how its tools support compliance with emerging cybersecurity frameworks like CISA's new guidelines.

About TrustInSoft
TrustInSoft is a leader in advanced software analysis tools and services that specializes in formal verification of C and C++ source code to ensure safety, security and reliability.

Media Contacts:
USA
Gavin Hill at gavin.hill@trust-in-soft.com
or
Clive Over at clive@napierb2b.com
Phone: +1 650-741-0004

EMEA
Natasha Henderson at natasha@napierb2b.com
Phone: +44 (0)1243 531123

Clive Over
Napier Partnership
+1 650-741-0004
email us here
Visit us on social media:
LinkedIn
YouTube
Facebook
X