Contribution ID: **87** Type: **Oral Presentation**

A comprehensive initiative to enhance the security posture of open-source software (Remote Presentation)

Tuesday, 26 March 2024 11:20 (20 minutes)

Protecting information assets has become a top priority for organizations in the ever- changing landscape of digital security.
INFN is deeply committed to security, being a major player in the research world with distributed computing infrastructures across the entire territory and being involved in numerous research projects that deal with health and sensitive data.
The Datacloud project aims to develop a portfolio of IaaS and PaaS cloud services, that will allow research partners to deploy innovative services by easily and transparently accessing geographically distributed computing and storage resources.
The middleware developed by Datacloud reflects the uniqueness of our technology compared to common public clouds in the market: our core strength lies in the middleware and cloud-native applications tailored to the needs of research communities and our ability to co-design solutions with our research partners.
Considering this, we are currently undertaking a comprehensive and strategic initiative to assess and enhance the security posture of our open-source components within the Datacloud production middleware. This middleware encompasses Platform-as-a-Service (PaaS) Orchestration system, Identity and Access Management (IAM), and TOSCA-based services.
Over the years, the accelerating pace of software development has, at times, led to security aspects being overshadowed in favour of expeditious feature releases.
Recognizing this oversight from the past, we intend to correct the situation, reinforcing security as a fundamental pillar in the development lifecycle.
The initiative is motivated by a compelling need to align with best practices and industry standards, namely the OWASP SAMM (Software Assurance Maturity Model) and ISO/IEC 27002 frameworks. The collaboration of these frameworks serves as the foundation for a robust and harmonized security posture. OWASP SAMM provides a maturity model specifically tailored for software security assurance programs, offering guidance on creating and evolving an organization-wide software security initiative. ISO/IEC 27002, on the other hand, focuses on information security management, providing a comprehensive set of controls and guidelines.
We acknowledge the need of a collaborative effort within our organization, which will actively involve development leads, “security champions”, and other key stakeholders.
We have identified a set of tasks to be implemented to establish virtuous processes aimed at enhancing our security posture.
In the initial phase of the plan, we will focus on the definition of security standards and policies, roles and responsibilities, and security training and awareness. The overarching goal is to create a robust governance framework that permeates the entire software development lifecycle.
Following that, the plan delves into the security self-assessment, which involves creating a comprehensive projects inventory and the initiating an evaluation and improvement plan. This stage integrates code reviews and initial implementation strategies, acknowledging the importance of automated security checks, continuous assessment, and code quality reviews.
A subsequent focus will be on setting up continuous monitoring processes to establish and maintain frameworks and processes for ongoing control and enhancement of software quality. This includes proactive measures for timely updates of dependencies and swift responses to emerging vulnerabilities.
This contribution will provide an overview of this pragmatic roadmap for realizing a more secure and resilient software ecosystem, ultimately leading to the implementation of inherently secure end user services tailored to scientific data analysis.

Primary author: ANTONACCI, Marica (INFN)

Co-authors: DONVITO, Giacinto (INFN); MARTELLI, Barbara (INFN - CNAF); CIASCHINI, Vincenzo (INFN

CNAF)

Presenter: ANTONACCI, Marica (INFN)

Session Classification: Network, Security, Infrastructure & Operations

Track Classification: Track 7: Network, Security, Infrastructure & Operations