Trusted CI Success Story
Custos

Trusted CI helps Indiana University's Custos Protect Science Gateways

Science gateway projects often have limited resources to devote to cybersecurity mitigation and are potential targets of cybersecurity threats. Without proper security, a scientist or student could lose years of research, or a university could owe millions of dollars to a ransomware threat.

As part of its mission to enable trustworthy scientific research, Trusted CI collaborated with Indiana University to assess the security of Custos, designed by the Cyberinfrastructure Integration Research Center (CIRC) to protect science gateways. "The engagement was immensely useful for us, and we appreciate the effort that went into this," said Marlon Pierce, principal investigator of the Custos award.

A single, open-source software solution that addresses the specific security requirements of science gateways, Custos offers an integrated approach to authentication, authorization, user management, group and role management, and security credential management.

Indiana University's Sample Gates

To conduct an in-depth assessment of Custos, Trusted CI applied the First Principle Vulnerability Assessment (FPVA) methodology. The first step was to map out the architecture and resources of the system, paying attention to trust and privilege used across the system, and identifying the high value assets in Custos. Next, Trusted CI performed a detailed inspection of the parts of the code that have access to the high-value assets.

Trusted CI's FPVA evaluation involved five steps.

- Architectural analysis: determine the major structural components of the system and how they interact
- Resource identification: identify key resources accessed by each component, including files, databases, logs, and devices
- Trust and privilege analysis: identify trust assumptions about each component
- Component evaluation: examine relevant components guided by high-value targets identified in the first three steps
- Dissemination of results: produce a final report with deliverables and recommendations

Trusted CI found serious security vulnerabilities as part of the evaluation, which have now been resolved. "We greatly appreciate the due diligence. This is an incredibly useful analysis for our group, the first of its kind. We also hope to cultivate some of the lessons learned in other software products we develop," said Suresh Marru, research scientist at Georgia Tech and former deputy director of CIRC.