Trusted CI Success Story
Tapis

Tapis more secure following Trusted CI code-level review

In 2023, the Texas Advanced Computing Center (TACC) collaborated with Trusted CI, the NSF Cybersecurity Center of Excellence, to assess the security of its Tapis software.

The Tapis Framework provides a hosted, unified, web-based application programming interface (API) for securely managing computational workloads across institutions. Tapis capabilities include cloud computing, identity management services, federated and local authentication, role-based authorization, secret storage, and security logging. The aim of the Tapis software is to enable experts to focus on their research instead of the technology needed to accomplish it.

Trusted CI performed a code-level security audit of the Tapis software, looking for weaknesses that could be exploited. The effort focused on core Tapis services responsible for accessing high-powered computing resources such as systems, apps, files, jobs, security, and the authenticator.

To conduct the assessment, the Trusted CI team applied its First Principles Vulnerability Assessment (FPVA) methodology. The analysis started by mapping 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 the system. From there, Trusted CI performed a detailed code inspection of the parts of the code that have access to the high-value assets.

Tapis is a collaboration between the Texas Advanced Computing Center at the University of Texas, Austin, and the ITS-Cyberinfrastructure group at the University of Hawaii and is funded by the National Science Foundation.

The Trusted CI team found four serious security vulnerabilities and one bug in the Tapis code and made several recommendations to the Tapis team to further increase security based on findings from the assessment, including:

- Regular assessments of the software to help maintain security
- Attention to the security of external software on which Tapis depends
- Regular database cleanups to discard malicious input
- Run stress testing scenarios to explore the maximum number of job requests and application containers that can be submitted and launched respectively at a time

After being notified of a Tapis vulnerability, Richard Cardone, a research associate at TACC, praised Trusted CI for its positive impact on Tapis security. “You guys caught a whale! The fix will go in as an emergency patch immediately. I alerted the rest of the team to check their code for the same problem. Great work!”