NIST Position Paper: Area #1

GitLab comments on the *Criteria for designating "critical software"* in support of the May 12th 2021 Executive Order on Improving the Nation's Cybersecurity, drafted May 26th, 2021.

> *Criteria for designating "critical software"*. Functional criteria should include, but not be limited to, level of privilege or access required to function, integration, dependencies, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised. See EO Section 4(g).

GitLab is excited to partner with NIST and other federal cyber stakeholders on Standards and Guidelines to Enhance Software Supply Chain Security. As a company that holds transparency as a core value, we are happy to share our learned best software security practices to help influence standards that strengthen the cyber resiliency of federal agencies and the broader cyber community.

The foundation for defining *Criteria for designating "critical software"* should be risk. It is important to implement a formal risk-based methodology built on industry best practices and internal risk appetite to introduce layers of risk, and therefore layers of requirements. Not all critical software will have the same impact on an organization, therefore the same investment should not be required when securing those pieces of software. This approach will also encourage more thoughtful deployment design, as the more isolated the product is from critical data and systems, the less investment needed upon onboarding and as part of continuous monitoring.

Internally, GitLab employs a critical systems tiering methodology as part of our Security Operational Risk Management function. A higher tiered software is subject to more stringent onboarding and continuous monitoring requirements. Once onboarded, software is continually assessed as part of annual Business Impact Assessments and ongoing Vendor Security Reviews for changes in scope of services offered or internal deployment. If a software changes tier it is automatically subject to the new requirement set.

In addition to the functional criteria listed in the executive order, criteria for software that stores/processes/transmits classified data, holds credentials for other critical systems, performance of a function critical to confidentiality, and performance of a function critical to availability should also be considered. This should also apply to the accesses defined for developing and maintaining these systems, so adopting Zero Trust principles should be considered a part of the development process, particularly for any critical software.

Systems architecture sometimes describes systems as a collection of capabilities, but not how those capabilities interact with each other or the user. The more components that are integrated as "bolt-on" capabilities, the more critical software that has to be installed, managed, upgraded and operated. Again, using Zero Trust principles here is recommended.

In general, all of the above aspects have to be considered to provide a new perspective on risk profiling and therefore critical systems designation.

In Closing

GitLab appreciates the opportunity to offer these positions to NIST in relation to EO 14028. We have proposed approaches that have proven to be fruitful in the modern software delivery model.

Submitter:

- Johnathan Hunt
- VP of Security, GitLab
- jhunt@gitlab.com