NIST Position Paper: Area #5

GitLab comments on the *Guidelines for software integrity chains and provenance* in support of the May 12th 2021 Executive Order on Improving the Nation's Cybersecurity, drafted May 26th, 2021.

Guidelines for software integrity chains and provenance. See EO Sections 4(e)(ii, vi, and viii).

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.

Complete documentation of the software is needed for showing the integrity of a software product. This should include various features and functionality, and security implications of using the product. When one considers the amount of dependency that organizations have on CSPs (Cloud Service Providers), external software components, and the steps for the actual building of a final product, a modern software product requires detailed documentation. This should include documentation of the underlying architecture which its components may reside on, revisions and historical information of components that make up the product including external software components, and details about how the software is actually built. The emphasis should be on the software, the environment that the software resides in, how the various components interact, and how the software is assembled together (the build process) into its final form.

This documentation should be a living document that is continually updated, as GitLab exemplifies with our product documentation site: docs.gitlab.com. It should be reflective of traditional "release notes" that often come with new software releases, but should also be reflective of the aforementioned infrastructure and build process. Changes and upgrades to such items as software components should be included as a part of this documentation process.

All software development organizations should have a vulnerability disclosure program. This should include a publicly documented way that allows people outside of the organization to report security vulnerabilities, and should include a stated method of how their disclosure process should work. While some smaller organizations may be able to handle this with a published process and a "security@" email address, for larger and more complex organizations the participation within a Bug Bounty program is recommended. This allows an organization to scale this process much more effectively. Additionally, vulnerability fixes should be prioritized accordingly to deliver critical patches and fixes to be applied to systems immediately. The process should also drive an underlying simplification of software components and development.

In general, with this level of documentation and the ability for a software developer to receive and act upon vulnerability reports, that software developer can more quickly assign resources where they are needed, whether this requires temporary or permanent adjustments to the infrastructure, contacting and working with outside developers that wrote and are responsible for externally-sourced software components, or regular internal coding changes.

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