ASWF Security Working Group

Charter Outline

Purpose

Focal point and cross functional group for security aspects of hosted projects at the Academy Software Foundation.

Goals

- Provide guidance/support/infrastructure to Academy Software Foundation hosted projects as they address OpenSSF Best Practices badge requirements.
- Education to studios, vendors, and other relevant organizations in the VFX industry on secure development and security best practices as it relates to projects hosted at Academy Software Foundation.
- Collaborate with industry groups such as MovieLabs and OpenSSF as it relates to the goals (such as with white papers, cross group participation, leveraging resources).
- Ensure LFX Security is used by all our projects, and help engage LFX Security product team to help evolve the tool for our projects.

Non-goals

- General education on security and secure development best practices to the VFX industry as a whole.

Deliverables

- Maintain OpenSSF Best Practices badge requirements documentation for those requirements for Academy Software Foundation projects, as well as upstreaming Academy Software Foundation use-cases to the best practices badge program.
- Develop policy for binary artifact publishing, including supply chain and signing.
- Develop plan for managing CVEs and security vulnerability management for hosted projects.
- Documentation on best practices in implementing Academy Software Foundation projects securely.
- Security tooling documentation for Academy Software Foundation project.
- Collaborative whitepaper with MovieLabs and OpenSSF on security topic relevant to the VFX industry.

Meeting Notes

08 February 2023

Video Conferencing Link

Attendees

- Jean-Francois Panisset (VES Technology Committee)
- Jean-Christophe Morin
- Larry Gritz (Sony Imageworks)
- Kerby Geffrard, OpenRV
- John Mertic, Linux Foundation
- Scott Wilson, Rust WG

New items

- Kerby: takes care of security on OpenRV, interested in the topic
- Scott: interested in security
- Jean-Christophe: on the Rez TSC, contribute on OTIO, participate in other ASWF activities. Interested in security, get security training from my employer. Also do a bunch of work on builds.
- Larry: software architect at Imageworks. Involved with several ASWF group: OSL, OpenEXR, mostly know the common sense security stuff, mostly an observer, hope to be a consumer of what comes out of this group
- Larry: many developers inside studios have never had to deal with these issues, running inside the firewall, running on trusted inputs from inside the studios. So never had to think about these issues, and seeing the requirements for an ASWF projects can be a surprise. Developers don't see themselves as experts, these are new design goals, and how do I get started. Here are new factors you need to consider.
- Scott: all devs in M&E, not just in studios, what Larry said is 100% valid, but for everyone in our space. Studios, vendors, etc.
- JC: do we want to produce material that is consumed by others, or more we reword things in ways that are simpler for projects to digest? Do we concentrate ourselves more on the ASWF projects, or the education side for the entire industry. And do we need to consider the entire industry as in scope? What does it bring compared to other security focussed education groups.
- JF: I feel our scope should be ASWF projects only.
- Scott: MovieLabs has a wider scope, there are other organizations. JF: there's also TPN, CDSA
- JC: concentrating on software security at first
- Scott: yes that's a good boundary at first. We don't have expertise on physical security for instance. But we have something to offer in terms of how write secure code, or in the case of OpenCue, how do you make that secure.

- JF: also in scope maybe is build security and supply chain: need to guarantee that people consuming our artifacts are secure
- JC: is licensing part of this? John: can be, where does the code come from. But licensing is tricky, "I'm not a lawyer and I don't give legal advice". So we can't give anything that seems like legal advice. So we don't need to build that expertise, there are outside groups that would be better resources and could get us away from liability. JC: makes sense, was just wondering if licensing was in scope, but wasn't arguing it should.
- Scott: what do we want to do about CVEs, would that still a responsibility for each project, or would this WG be part of this? John: a good question. JC: come up with a plan for projects for how they can accept CVEs, communicate them so it's easier for projects to deal with them. JF: recommend to projects that they enable and use the GitHub functionality for reporting security issues and dealing with CVEs. JF: could add language in projects requirements about suggesting using GitHub for reporting, and add language about CVE handling.
- John: we do have Snyk available, but doesn't deal with C/C++ projects? JC: yes, it does since mid 2022. Not supported for automatic scanning https://docs.snyk.io/scan-application-code/snyk-code/snyk-code-language-and-framework-support but supported if you set it up manually.
- https://docs.snyk.io/scan-application-code/snyk-open-source/language-and-package-manager-support/snyk-for-c-c++
- Scott: we could produce documentation for new ASWF projects, here's information on how to bring up your security level, but can also be used externally by non-ASWF projects.