Open Horizon project
TSC Meeting

November 7, 2022

THE LINUX FOUNDATION

LF EDGE

Meeting Details

Time: November 7, 2022 11:00 AM Pacific Time (US and Canada)

Please download and import the following iCalendar (.ics) files to your calendar system.
https://zoom.us/meeting/tJMrce2hqTIjHNa60DHyv9sn847QK4LGK_Gf/ics?icsToken=98tyKuCvqD0uE9OcuR-FRowEBI_oLPPwtlhEgo1cyk_BKzlFOxD4brYVA5krPP_7

Join Zoom Meeting
https://zoom.us/j/97664979962?pwd=TlY3dUk4K0Y3WnZXMjVMeisreGRkQT09

Meeting ID: 976 6497 9962
Passcode: 312515

Find your local number: https://zoom.us/u/ac5YZ6pqGW

LF Antitrust Policy Notice

Linux Foundation meetings involve participation by industry competitors, and it is the intention of the Linux Foundation to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of, and not participate in, any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

Examples of types of actions that are prohibited at Linux Foundation meetings and in connection with Linux Foundation activities are described in the Linux Foundation Antitrust Policy available at http://www.linuxfoundation.org/antitrust-policy. If you have questions about these matters, please contact your company counsel, or if you are a member of the Linux Foundation, feel free to contact Andrew Updegrove of the firm of Gesmer Updegrove LLP, which provides legal counsel to the Linux Foundation.

Open Horizon TSC

Working Group or Partner	Representative
Agent	David Booz
DevOps	Ben Courliss
Documentation	Joe Pearson
Examples	Troy Fine
Management Hub	Nathan Phelps
Outreach	Susan Bowlin
Partner: mimik Technology	Michel Burger
Partner: Accuknox	Rahul Jadhav
Partner: IBM	Kavitha Bade

Announcements

THE LINUX FOUNDATION
LF EDGE

OpenSSL Critical Vulnerability, Downgraded to High

OpenSSL initially posted that researchers had uncovered a critical vulnerability, and that everyone should be prepared to address when the CVE will be issued and the vulnerability detailed on November 1. *Joe notified TAC and Project Lead mailing lists and requested response from TSCs.*

- CVEs were High, not Critical: https://www.openssl.org/news/vulnerabilities.html#CVE-2022-3786
- Announcement: https://mta.openssl.org/pipermail/openssl-announce/2022-November/000241.html
- Release Notes: https://www.openssl.org/news/openssl-3.0-notes.html

Project Status relating to CVEs (links to vulnerability disclosure page)

- Akraino: Security subcommittee will look into it for each blueprint
- Baetyl:
- EdgeX Foundry: believe not affected and so fixes are not needed. The Kong instance does not request client authentication and the issue only affects openssl 3.x branches which are not used by our (alpine) base images
- eKuiper: no fixes needed – do not use OpenSSL in source or v3 in containers
- EVE: no fixes needed - debug container uses v1.1.1, GoLang TLS
- Fledge: no fixes needed - we only use v1.1.1
- Home Edge:
- Open Horizon: fix likely not needed - Exchange container uses UBI, will rebuild out of caution when UBI 9 released, GoLang TLS, updated SECURITY.md
- Project Alvarium: no known direct dependency on OpenSSL, possibly golang:1.17-alpine for scoring apps
- Secure Device Onboard: no immediate impact to FDO. OpenSSL 3 not used. WIll upgrade to 3.0.7 later.
- State of the Edge:

What are projects responsible for? What should TAC do?

All: Work towards meeting questions in OpenSSF Best Practices.

- There MUST be no unpatched vulnerabilities of medium or higher severity that have been publicly known for more than 60 days.
- Projects SHOULD fix all critical vulnerabilities rapidly after they are reported.

Impact Stage: "**Establish a security and vulnerability process**"

- Akraino:
- EdgeX Foundry: wiki - SIR team, reporting process, response process, list of known issues
- Home Edge: Posted a SECURITY.md policy in GitHub listing vulnerabilities, reporting process and responses.
- OH: Security Team, private mailing list for publish submissions, SECURITY.md file in .github repository, adding known vulnerabilities page to documentation site.

Open Horizon's response to OpenSSL Vulnerability

- Held first meeting (not in public) of WG leads as security response team.
- Formulated plan of action to address:
  - Roughed out plan with contingencies based on best guesses until CVE issues
  - Investigated source code and containers
  - Determined no direct usage of OpenSSL libraries, used GoLang implementation
  - Determined UBI container should be refreshed
  - Created site-wide security policy in GitHub
  - Created publicly-available private mailing list for vulnerability submissions
- Overall, it was an effective and quick response. How can we improve on it?

Transitioning from Akka (to Pekko?)

- Akka is moving to a BSL 1.1 software license next year, which is incompatible with Linux Foundation projects.
- Nathan Phelps has looked into alternatives. What is the current status and next steps?

Working Group Updates

THE LINUX FOUNDATION
LF EDGE

Next Meeting

THE LINUX FOUNDATION
LF EDGE

Next Meeting

- Next Meeting: Monday, December 5 @ 11:00am PT/02:00pm ET
  - November 21 is Thanksgiving week, are most people out?

Thank You

THE LINUX FOUNDATION
LF EDGE

Repositories per Working Group

Agent	DevOps	Documentation	Examples	Mgmt Hub
anax edge-sync-service edgeengine-integration edge-sync-service-client rsapss-tool mms-cloud-container	devops horizon-deb-packager edge-utilities	.github artwork open-horizon.github.io documentation-migration project-summary	examples open-horizon-services	exchange-api SDO-support vault-exchange-auth