CSIRT Tooling: Best Practices in Developing, Maintaining and Distributing Open Source Tools

or are we really following our own advices?

CIRCL
Computer Incident
Response Center
Luxembourg

Team CIRCL *TLP:WHITE*

08th November 2018

Context

- As CSIRT, we are developing **more and more tools** (software, hardware) to support our activities.
- In the scope of CEF Generic Services, CSIRTs develop, release and maintain open source tools which are used at national, european and international level.
- CSIRTs should provide **a good example in the security field** to the community at large when releasing open source tools.
- There is **no official directory of open source tools** developed maintained by CSIRTs.

Outcome

- We decided to write a document from scratch to document the best practices when developing, maintaining and distributing open source tools.
- The document is a **collaborative effort** within the CSIRTs network (CIRCL, CERT.at, ANSSI-FR, GOVCERT.LU and CERT-EU already contributed).
- The document is written in markdown format and accessible via GitHub.
- The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119.

Software Development Practices

- CSIRT tooling must have at least one (open) source control management repository (if the project is larger, multiple repositories might be required).
- CSIRT tooling repository must be publicly accessible.
- CSIRT tooling repository must allow external contributors to propose changes (via pull-request) and open issues easily.

Security Vulnerabilities and Software Assessment

- CSIRT tooling must have at least a specific point-of-contact for security vulnerability notification with an associated PGP key.
- CSIRT tooling must provide a way to assign CVE in case of discovered vulnerabilities and provide a fix in a timely scope.
- CISRT tooling must have a vulnerability disclosure policy.

Open Source Software License

- CSIRT tooling must be licensed under an approve open source license[1] [2].
- CSIRT tooling must regularly review the license compatibilities with dependencies.

[1] https://www.gnu.org/licenses/license-list.en.html

[2] https://opensource.org/licenses

Privacy and Personal Data Processing

- CSIRT tooling should include a description of the information which has a privacy impact and how to improve privacy when deployed.
- CSIRT tooling should include functionalities and technical measures in order to improve privacy.

Contribution and Collaboration

- CSIRT tooling should include a code-of-conduct such as Contributor Covenant Code of Conduct[3].
- Chat channels and/or mailing lists help with empowering a community[4].

[3] https://www.contributor-covenant.org/

[4] Social Architecture, Pieter Hintjens
http://www.foo.be/docs-free/social-architecture/main.pdf

Interoperability

- CSIRT tooling should have an open and documented API to interact with tools (such import/exporting information, triggering operations of the CSIRT tooling).
- CSIRT tooling may publish their format specifications to a standard organisation such as IETF, ITU or OASIS.

Directory - CSIRT tooling

Software	CSIRT lead
MISP	CIRCL
AIL	CIRCL
BGP Ranking	CIRCL
cve-search	CIRCL
IntelMQ	CERT.at
n6	CERT.pl
TheHive	BDF CERT
Cortex	BDF CERT
eml-parser	GOVCERT.LU
bmc-tools	ANSSI-FR
bootcode-parser	ANSSI-FR
bits-parser	ANSSI-FR
AD-control-paths	ANSSI-FR

Next steps

- **Gap analysis of the recommendations** for each CSIRT tooling listed to help maintainers to achieve a certain level.
- Generate and publish a public directory of the CSIRT tooling with their scope.
- Review the current state of the tooling (such as new tools, interoperability with existing one, documentation or security assessment) within the CSIRT networks and propose action plans to have more **coordinated approaches in development and maintenance**.

- `https://github.com/CIRCL/compliance/tree/master/csirt-tooling-best-practices`
- `https://github.com/CIRCL/compliance/blob/master/csirt-tooling-best-practices/csirt-tooling-best-practises.pdf`
- Document is also published in the CSIRT network portal in the Tooling WG.
- We welcome pull-request(s) and contributions.