DPDK

Intro to the new DPDK Vulnerabilities management process

Maxime Coquelin

DPDK Userspace – Bordeaux – 2019

Background

- DPDK is a sensitive piece of software
  - Used in telecom infrastructures, public Clouds, ...
  - Interfaces sometimes exposed to untrusted sources
    - e.g. Vhost-user lib with untrusted guests
- Until now, no formal process defined
  - Who should I contact when I find a possible vulnerability?
  - Is it really a vulnerability or just a bug?
  - Who should work on fixing/reviewing it?
  - How to release the fix?

Background

- One CVE in 2018: CVE-2018-1059
  - Managed to get if fixed
  - But lots of questions raised
- The Technical Board decided it was time to define a formal process
  - Inspired by the processes from OVS, FD.io and others.
  - Reviewed by members security teams (e.g. Intel, Mellanox, Red Hat)
  - Voted by the Technical Board
- http://doc.dpdk.org/guides/contributing/vulnerability.html

Reporting a vulnerability

- https://core.dpdk.org/security/
- Do **not** use Bugzilla to report any possible vulnerability
- Send an e-mail to security@dpdk.org
  - Use GPG to encrypt the mails (Initial reporting and further communications)
  - Security team members: Ferruh Yigit and Thomas Monjalon
- Unsure this is a vulnerability? Consider it is one and follow the process!

Reporting a vulnerability

- The report should contain
  - Detailed information about the vulnerability
  - A reproducer (if available)
  - The fix (if available)
- But also
  - How the reporter wants to be credited
  - Preferences about the embargo duration (if any)

Vulnerability confirmation

- The security team reviews the report, involving area experts if needed
- If the vulnerability is not confirmed
  - Request the reporter to report the issue using the usual channels (Bugzilla)
- If the vulnerability is confirmed
  - Affected DPDK versions assessment
  - Bugzilla ID allocation from dedicated pool
  - Security score calculation using CVSS Calculator
  - Define embargo duration (if any)
- Confirmation e-mail sent to the reporter with above info within 3 business days

CVE request

- DPDK project is not a CNA (CVE Numbering Authority)
  - Security teams requests a CVE number to a CNA
  - Currently using Red Hat as CNA
  - But Techboard request for Linux foundation to become one
- Security team uses pre-defined template for its request
  - Description
  - Severity score
  - Embargo duration
  - …

Fix development & review

- This step may be started in parallel of the CVE request
- Fix implemented by the Security team and/or elected area experts
  - Impacted component maintainer
  - Regular and trusted contributor
- Backport to affected stable version is also prepared

Pre-release disclosure

- Pre-release disclosure of the security advisory and patches
  - Usually one week before end of embargo
  - Signed with a security team member GPG key
- Goal → let time for downstream stakeholders to prepare new releases
- Who is eligible?
  - Operating Systems vendors
  - Major DPDK users
- How to apply?
  - Send request to the Tech Board (techboard@dpdk.org)

Public disclosure

- End of the embargo
  - Patches are pushed to master and stable branches
  - New versions of the stable branches released
  - Reserved Bugzilla is filed with the security advisory
- Advisory sent to announce@dpdk.org
- Patches posted to dev@dpdk.org

Questions?

Maxime Coquelin

maxime.coquelin@redhat.com