THALES

Revalidation in response to CVE
CMUF working group

Fabien Deboyser
ICMC 2017 – May 18th 2017
C22c

Background

- **ICMC 2016 presentation : "Reconciling vulnerability response with certifications"**
  - Needs of a dedicated framework in FIPS 140 for security updates
- **Working group creation after the ICMC**
- **Monthly meetings - 1 hour**
- **ICMC 2017 : working group status**
- **IG G.8 update?**

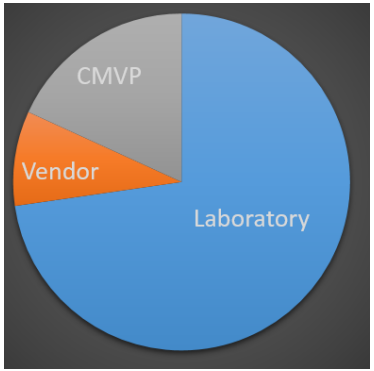
"Knowing is not enough, we must apply.
Willing is not enough, we must do"
Bruce Lee

Source wikipedia

Participants

Source unplash

- Acumen - Ryan Thomas & Ashit Vora
- Atsec - Renaudt Nunez & Yi Mao
- CMVP - Carolyn French & Ryan Horan
- Cygnacom - Nithya Rachamadugu
- EWA - Richard Adams, John Kohnen & Jesse Wood
- Thales - Fabien Deboyser



Context

Security vulnerability are "issued" and "publicly disclose"

- "urge" for developer to analyze and respond to it (communication/update)
- Update is done but customers can't use it until certification granted, meanwhile product vulnerable

Internal security vulnerability

- FIPS 140-2 process (IG G.8) is not optimum and not in favor of the disclosure of a security vulnerability and **do not reflect the importance of the needs of an update** (item can be categorized as 1SUB only)
  - 1SUB for non-FIPS relevant
  - 3SUB if FIPS security relevant – but similar to "recertification" with potential new hw/sw/fw less than 30% of FIPS relevant
  - 5SUB if FIPS security relevant with a different lab

Certification is a market differentiator & required for/by customers

- Need the right trade-off between certification and security
- Security with a certification that adapts to its speed
- IMHO it is in favor of certification to value security
- NIST "favors" using latest security version over the latest certified one with bugs ….

Source pixabay

Please close your eyes !!

Quick overview of the IG G.8

Scenario 1

- administrative update
- hw/sw/fw modifications but no FIPS 140-2 relevant items
- either functionality that it was impossible to test OR security relevant function that was in the scope but not tested

Scenario 1a

- rebranding of an OEM no modifications
- ported sub-chip cryptographic subsystem

Scenario 1b

- CST lab performs a revalidation for a validated module and this lab was not the original lab performing the original evaluation

Scenario 2

- ~~Not use then for us? ☺~~

Scenario 3

- modifications that affect some of the hw, sw or fw components FIPS security-relevant (with a limit of 30%)

Scenario 4

- modification of the physical enclosure, no operational changes to the module
- (I assume purely hardware)

Scenario 5

- hw/sw/fw modification that do not meet the previous conditions
- + scenario 3 with a different lab

Proposal by the working group

Propose an update of IG G.8 for an update of a public vulnerability

Define IAR template as suggested originally and now in the IG G.8:

- Precise activities to be done for the revalidation (submission from dev to lab and lab to CMVP)
- Rationale over the TE + Presentation of the update

Proposed update of IG G.8

Modifications are made to the sw/fw on FIPS security relevant items with the following conditions:

- The required update comes from a publicly disclosure vulnerability (CVE, other)
- The update is only concerning the published publicly disclosure vulnerability ~~less than 2% of security relevant~~
- ~~Note that the lab have the discretion of validating that this can be "applicable"~~

Discussion highlights :

- CMVP is interested and receptive
- Dedicated Submission (new 1C? Or using the current 2SUB and move the 2 SUB to another one)
- To be included in G.8
- How to reflect the version with a certificate? Creation of a Certificate caveat?

Next steps:

- For all the "?" on the proposition further analysis needed
- Work on the wording in a "G.8" fashion ~~and propose it to the group before next meeting~~
- Next meeting the 12~~th or 13th of April~~

Discussion extracts

"I am still not convince that listing the CVE in the SP is the right approach.. It will open door to have formal approval by the lab that all the latest CVE are listed.. Although listing the reason of the update may be a good approach"
Fabien Deboyser

"We don't need any measurement except the precise CVE"
Carolyn French

"We need a good product versioning for FIPS"
Renaudt Nunez

"Needs to be short and few testing ☺"
Carolyn French

"We would rather call it management of vulnerability"
Nithya Rachamadugu

Source unplash

THALES

Proposed update of IG G.8 in detail

- IAR (CC wording) from the developer -> **based on a template**
  - Identification of the vulnerability + modules (versions + references CAVP, CM certificates…)
  - Source code review against the original certified (can be done with screen capture)
  - Analyze what TEs are impacted (regression table G.8)

- Report from the lab -> **based on a template**
  - Analyze the TEs -> regression testing based on G.8 (relevant subset?)
  - Description of the updates
  - Runtime validation of the product
  - Functional testing or algorithm testing? (needs to be performed?) **Not**

- SP update
  - Update of the sw/fw reference
  - The vulnerability to be listed in an appendix of the SP?
    We want to catalize the customer to update quickly but there is not universal agreement on what it will look and what information will be shared

- Certification status
  - Implied that previous certification is no longer valid.
    TBD because some mitigation can be done (deactivation, operational, …) and then not necessary to FIPS update

- Sunseting policy, no extension of the validity

THALES

Thank you!!

Fabien Deboyser

Security Certification Engineer

Thales e-Security - Plantation Florida

Fabien.deboyser@thalesesec.com