Table of Contents

EMI Updates Process

EMI Products Release Categories

An EMI distribution includes all the products that are developed within the project and that have reached production quality. Within an EMI major release, only one major version of a given product is maintained.

- the different types of EMI release are defined in the Change Management Policy

EMI Versioning schema

For products releases, EMI is adopting, as VERSION-RELEASE numbering convention, the typical **major.minor.revision(-[age/release])** schema, where:

- increment in *major* number reflects a change in the component interface or behavior, that can be backward-incompatible;
- increment in *minor* number reflects a change in the component interface or behavior backward-compatible. It can include also bug fixes.
- increment in *revision* number reflects bugs fixes, with no new features;
- increment in *age* number reflects a rebuild due to change in the external dependencies or an emergency release for component-x.y.z, when the version component-x.y.z+1 is already available.

source EMI Release Plan

EMI Updates Versioning schema

The EMI 1 Udpates are named as *"EMI 1 (Kebnekaise) Update X"*. For the moment EMI provided the emi-version package containing the */etc/emi-version* file:

```
# cat /etc/emi-version
1.1.2-1
```

This versioning follows the standard VERSION-RELEASE convention, in the sense:

- increment in *major* number reflects a EMI major release;
- increment in *minor* number reflects the presence in the corresponding Update of at least one product minor update;
- increment in *revision* number reflects the presence in the corresponding Update of products having only revision updates

EMI Updates Schedule Methodology

The Updates process consists of:

- **planning** - during the EMT weekly meetings:
  - pre-requirement - **ALL** requests for changes (GGUS tickets, internal defect, planned or unplanned improvements) should be tracked in PTs tracking systems, having an agreed Priority or in the EMI development tracker - see Change Management Policy - RfC handling for more details.
  - if a PT has **external contributions** and wants to release within EMI new functionalities requested outside EMI, they are accepted upon timely notification, so that the impact of the change can be understood. The changes will be released, but not supported, in EMI if the EMI

QA policies are followed. A Note is added on the Release Notes "External Contribution, released in EMI, not supported by EMI"
    - EMT metrics reports provided by SA2.3 team containing:
        - untouched & accepted immediate/high priority RfCs, are discussed and PTs provide a date for implementing the fix or feature
- **scheduling**:
    - There will be **NO** Update containing **ONLY** *Medium* or *Low* priority components RfCs. In other words: there will be **NO** Update if there are no Immediate or High priority RfCs or components Minor releases.
    - a task for each component to be updated is opened in the EMI Release tracker that will track all the RfCs intended to be addressed by this new Component Release (CR). See Change management Policy - CR handling for more details.
- **development/fix implementation/testing/certification** - PTs follow EMI Release Checklist - when this stage finishes the CRs tasks become `Certified`
- **validation/testbed deployment/verification** - once certified, the QC team starts the verification step - see details at Release Task state transition diagram
- **Update preparation and deployment** - see EMI Update Preparation Checklist for more details.

EMI Updates Schedule details

We will have a three-week release cycle:

- 1st Monday (Mo1)
    - tasks that are at least in the `Certified` status are considered to be released at the end of the cycle
    - `Certified` tasks pass through the first SA2-QC verification phase to the "Ready for Testbed" status
- 1st Thursday(Th1)
    - prepare deployment repository and an EMI-EMT task, category "EMT testbed", is created to follow-up the deployment on the testbed of verified tasks
- 2nd Monday (Mo2)
    - status of the deployemnt is presented during the EMi-EMT weekly meeting
    - eventual last-minute Certified products are added to the Update
- 3rd Monday (Mo3)
    - status of the deployed products and of the QC final verification are evaluated
- 3rd Wednesday (We3)
    - finish EMI testbed testing
    - last final QC verification reports available
- 3rdThursday (Th2) - analyze verification and testing results, finish EMI Update Preparation Checklist
    - products not meeting the Production Release Criteria are rejected, their tasks return to "Open" and it will follow another release cycle, once *Certified* again.
    - Announce the Update
- following week is used for SA1 activities, testbed setup, internal NAGIOS monitoring.

Emergency Updates

Emergency Updates are a special case of Updates containing only Immediate priorities RfCs that need to be addressed ASAP

- A RfC and a corresponding CR are created in the respective trackers;
- The problem is analyzed and an Immediate priority is assigned by the PT to the RfC
- RM prepares a detailed report containing the assessment of the priority done by the PT and his/her recommendation and sends it to the PTB for approval and endorsement. A minimum one working day time slot is required to receive the decision.

- Once a decision is taken it is communicated to the involved PT.
- If approved the current Update cycle is blocked and PT/SA1/SA2 work to provide the solution ASAP.
- An Emergency Update cannot be done concomitant with a Normal Update
- PTs/SA1-teams follow the EMI Release Checklist to deliver the fix

Addressing Security Vulnerabilities: -

- for Security Vulnerabilities assessed as such by the EGI-SVG:
  - for **LOW** (target date = 1 year) & **MODERATE** (target date = 4 months) risk assessment - issues will be threated as a normal RfC to be addressed in one of future updates of affected products, to be made available through a normal EMI Update, by the "due date" mentioned in the assessment
  - for **HIGH** (target date = 6 weeks) risk assessment - issues will be further assessed, together with EGI-Operations taking in consideration the impact on the production-sites/users. In case it is evaluated as **CRITICAL** risk (target date = 3 days) the **EMERGENCY** procedure for an Immediate priority RfC must be followed. Otherwise: if by the "due date" it is available a normal EMI Update Cycle, the issues should be threated as a High priority RfC to be fixed by an update of the affected product through the first normal update cycle; if by the "due date" there is no normal EMI Update Cycle, the issues should be threated as an Immediate priority RfC to be released following the **EMERGENCY** procedure.
  - for **CRITICAL** (target date = 3 days) risk assessment - the **EMERGENCY** procedure should be followed.

- RfC for security vulnerabilities:
  - in case of security vulnerabilities assessed as such by the EGI-SVG or by the PT itself - the RfC must reference the EGI-SVG internal, private, RT tkt. No description or details regarding the vulnerability should be present in publicly available places.

- Release Task Tracking:
  - Component Release Notes:
    - in case the updated product/component contains the fix for a security vulnerability the Release Notes/What's New section must contain the reference to the EGI SVG: Advisory, no other details regarding the vulnerability should be present.

Emergency procedure amendment:

- as EMI software code is open source and publicly avaialble any mention of "security vulnerability fix", "security", "vulnerability" & other exposes users/sites using EMI software that don't upgrade immediately there won't be any announcement of the release of the fixed product until the SVG-Advisory is send (made public) by the EGI-SVG. The availability of fixed product (packages) in EMI repositories with eventual Release Notes, in case aditional consifguration steps are needed, will be send to the EGI-SVG, through comments in the respective RT-tkt.
- when EGI-SVG issues the "*WHITE- Unlimited distribution allowed*" SVG Advisory (ref. 1) - EMI will announce its user-community through the usual channels - e-mail, web pages, RSS

- References:
  - Security Incident Handling Procedure
  - Vulnerability issue handling process

-- DoinaCristinaAiftimiei - 17-May-2011

This topic: EMI > EMIUpdatesSchedule
Topic revision: r29 - 2012-11-19 - DoinaCristinaAiftimiei