Security Coordination Group (SCG)

|  |  |
| --- | --- |
| **Venue:** | Telecon |
| **Date and Time:** | Wednesday 11th January 2012 at 10 CET |
| **Agenda:** | https://www.egi.eu/indico/conferenceDisplay.py?confId=742 |

Participants 2

MINUTES OF THE PREVIOUS MEETING 3

ACTION REVIEW 3

D4.4 STATUS & WRAP-UP and RISK REGISTER ROADMAP 3

Preparing for PY2 review 4

AOB 4

Actions 5

CSIRT REPORT 8

SVG Report 8

# Participants

|  |  |  |  |
| --- | --- | --- | --- |
| Name and Surname | Abbr. | Representing | Membership[[1]](#footnote-1) |
| David Kelsey | DK | EGI SPG Chair | Member |
| Linda Cornwall | LC | EGI SVG Chair | Member |
| David Groep | DG | EGI Representative in EUGridPMA | Member |
| Steven Newhouse | MM | EGI.eu Director and CTO  | Member (Chair) |
| Michel Drescher | MD | EGI.eu Technical Manager | Observer |
| Peter Solagna  | PS | EGI.eu Operations Officer | Observer |
| Tiziana Ferrari | TF | EGI.eu Chief Operations Officer | Observer |
| Damir Marinovic | DM | EGI.eu Policy Development Officer | In Attendance |

Apologies

Mingchao Ma

David O’Callaghan

Sven Gabriel

# MINUTES OF THE PREVIOUS MEETING

The minutes of the last meeting held on 10th October 2011 were reviewed. No other additions/corrections were reported. The minutes were approved as a correct record of the proceedings.

# ACTION REVIEW

SCG members and observers reviewed the SCG action list from the previous SCG meetings. Several actions were closed. See the table at the end of the minutes for more details.

TF: EGI security notice needs to be translated into official EGI policy. We have already information that WLCG have this policy. There is a need to consult the user communities and to produce the appropriate policy. DK: If we need policy, it should be a SPG policy. TF: To me it looks like SPG policy. DK: We should add this request to SPG agenda. Add as agenda point discussion about possibility to translate EGI Security notice to EGI security policy on next SPG face-to-face meeting ***(action 05/01)***.

TF: When we want to consult user communities what is the best way to get efficient feedback; through survey that is open or it is something that should go through the UCB? SN: What middleware components are proxy capable and which ones are not? LC: All middleware that need renewal, most can cope but I don’t have definitive answer. PS: 2 features are essential, capability to renew proxy and other one is automatic renewal. MD should contact the middleware providers and see which ones use proxies and what services are long running and need to deal with proxy related issues in terms or requiring middleware changes ***(action 05/02)***.

|  |
| --- |
|  |

# D4.4 STATUS & WRAP-UP and RISK REGISTER ROADMAP

SN: Thankful to LC for editorial and leading role. D4.4 gone to external reviewers and will be back for feedback to reviewers. Any other points SCG needs to consider and think about?

LC: SCG members should read the D4.4 one more time when we have a final version. Next thing is to do actual risk assessment. In this moment, we have 8 or 9 people subscribed to EGI Security Assessment Group. It is difficult to assess how much manpower will take for the assessment? SN: If you need more people we have mechanism to NGI International Liaisons (NILs) to try to gather more people. DK: Good idea, to get people from various NGI to do assessment. SN: Contact NILs to gather more people to join risk assessment exercise ***(action 05/03)***.

SN: Discussion on depth and timeline for risk assessment. We have annual review preparation and annual deliverables to finalise by the end of the April. We should start working on risk assessment and risk register as soon as possible. Because of time constraint, it makes sense to do quick exercise and then priorities areas we need to focus more and perform deeper assessment. We can present results to reviewers so they can assess whether it is sufficient enough. LC: According to the schedule it should be in the first 3 months. We should start the assessment in 1st quarter of 2012 without many difficulties. DK: Agree about quick scan I agree. On current list of people available there are all quite busy people. SN: We have MS224 Security Activity within EGI that DM will take editorial role; we need annual report from all EGI security groups. It is agreed that next steps are to have a call to have a new name, look at WSCLG risk register and do a quick scan. Eventually, we can start with partial work on deep scan and present it to the reviewers at the PY2 review.

|  |
| --- |
|  |

# Preparing for PY2 review

*Roadmap & status of of security related issues identified in PY1 review*

SN: We need formal response from SCG on security comments from PY1 review report; document on what we have done in response to their comments. DK: Some response already went out? SN: We provided some response in general, but we didn’t provide what we are going to do and what was actually done. DK: Major part of our response is in D4.4 SN: Yes, we just need to highlight certain parts in response to their concern. We don’t need to have a document right now but we need to prepare it in time for the PY2 review.

DK: What are the dates for PY2 review? SN: 27th and 28th June. We need to have Chairs of security groups available and present at the review event.

Concerning MS224 Security Activity within EGI, DM will get in touch with you and start collecting reports. We need to start review process about month from now ***(action 05/04)***.

# AOB

SN: Any written reports from Chairs? We need your written report but for today you can verbally inform us about your recent activities. Submit the report that will be included as integral part of this MoM ***(action 05/05).***

DG: Middleware providers 2 compability, you get modern hashes and proxies. LHCb framework cannot deal with modern proxies without removing old ones. The release of SHA-2 proxies may be delayed in 6 months time. SN: How much security risk differences there are between new vs. old hashes? DG: 80 bits of entropy are still OK. But we will have to SHA-2 once SHA-1 alg are broken. Don’t expect to happen this year. Security wise, we are OK. SN: We should pressure LHCb to get their framework update. DG: LHCb needs to be deal with modern proxies and it is not fault of dCache in this case. SN: Why are they are not reacting? DK: In this moment it is not a security issue, but it could become one. PS: At the beginning of December, when we were discussing dCache, they say that legacy proxies are supported by dCache DG: We cannot positively prove that they work together. It will take lot of engineering work for that. SN: We need to closely monitor and have a discussion with Ian Bird and Jaime Sheers about what is their understanding of priority in LHCb framework ***(action 05/06).***

TF raised a question about schedule for future releases, calendar and whether there is enough time for testing a new releases and preparation for it. It was agreed that TF and DG have discussion on this subject offline.

DK: Not a great deal happening for SPG side. On the next F2F meeting in Amsterdam, it is important to define work priorities for the 2012. For example on data protection we need to do more. There is ongoing work on revision of the Top-level Security Policy.

LC: Concerning SVG, January went quite smoothly. There was one release to fix one serious vulnerability. We need to improve and find a way a getting report metrics and numbers. Spanish will publish report and assessment; WMS review is to get done first.

Set up doodle for the next SCG meeting, to be held approximately in the middle of February ***(action 05/07).***

# Actions

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Resp. | Description | Status[[2]](#footnote-2) |
| 02/02 | JW | Circulate to the SCG list EMI faults on common security libraries  |  OPEN |
| 03/01 | PDT, SN | Define the distribution mechanism for sending policy drafts and define what mailing lists that should be included in consultation; discuss the proposal in Lyon |  CLOSED |
| 03/02 | DK, TF | Revisit the glossary and define the term Infrastructure |  CLOSED |
| 03/03 | MM, TF |  External RiP MoU should make it clear what is relationship between sites covered by MoU |  CLOSED |
| 03/04 | TF | To put in place MoU between EGI and Canadian sites in order to clearly define our relationship |  OPEN |
| 03/05 | SN | Contact Compute Canada CSIRT |  CLOSED |
| 03/06 | LC | Draft D4.4 ToC until end of August |  CLOSED |
| 03/07 | SN | Schedule SCG meeting in early September before TF in Lyon |  CLOSED |
| 04/01 | DK | Start Doodle on meeting availability for the F2F |  CLOSED |
| 04/02 | MM | MM to summarise and send to MD to bring short-lived credentials and lifetime of proxy certificates subject to the TCB-9 meeting |  CLOSED  |
| 05/01  | DK | Add as agenda point discussion about possibility to translate EGI Security notice to EGI security policy on next SPG face-to-face meeting | NEW |
| 05/02 | MD | Contact the middleware providers and see which one use proxies and need to deal with proxy related issues that require middleware changes | NEW |
| 05/03 | SN | Contact NILs to gather more people to join risk assessment exercise | NEW |
| 05/04 | DM | Contact Chairs of EGI security groups and start collecting reports for MS224 Security Activity within EGI | NEW |
| 05/05 | DK, LC, MM, DG | Submit the reports that will be included as integral part of this MoM | NEW |
| 05/06 | DG, SN | Have a discussion with Ian Bird and Jaime Sheers about what is their understanding of priority in LHCb | NEW |
| 05/07 | SN | Set up doodle for the next SCG meeting, to be held approximately in the middle of February  | NEW |

Minutes prepared by Damir Marinovic 11.01.2012.

Minutes Approved Group Chair Steven Newhouse

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

COPYRIGHT NOTICE

Copyright © EGI.eu. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs 3.0 Unported License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/3.0/ or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.

The work must be attributed by attaching the following reference to the copied elements: “Copyright © EGI.eu (www.egi.eu). Using this document in a way and/or for purposes not foreseen in the license, requires the prior written permission of the copyright holders. The information contained in this document represents the views of the copyright holders as of the date such views are published.

# CSIRT REPORT

There was not too much going on in December. The second release of security
dashboard was made just before Christmas. Some improvements have been made.
The development of security dashboard continue. It is expected in full
production in Q1 of 2012. In December, EGI CSIRT issued one security alert
and handled one security incident. EGI CSIRT had regular monthly meeting on
15th December ([https://www.egi.eu/indico/conferenceDisplay.py?confId=711](https://www.egi.eu/indico/conferenceDisplay.py?confId=711" \t "_blank)),
where CSIRT 2012 roadmap was discussed and thereafter was incorporated into
SA1.2 2012 roadmap, available at [https://wiki.egi.eu/wiki/Plan\_2012\_SA1.2](https://wiki.egi.eu/wiki/Plan_2012_SA1.2%22%20%5Ct%20%22_blank).

# SVG Report

12 new issues reported, including 3 which referred to software only having 1 instance (GGUS and Panda)  - which were fixed quickly without the need for an advisory.  4 advisories issued by SVG, 1 new issue lead to CSIRT advisory.

Improvement to handling of the issues, particularly ‘Low’ and ‘Moderate’ risk issues,  to ensure they don’t get forgotten and to know which issues are fixed in which version of the piece of middleware, which version of EMI, and which version of the UMD.

System for handling gLite 3.2 and gLite 3.1 security fixes between now and April 30th when security support ends agreed.  From now only ‘High’ and ‘Critical’ risk issues will be fixed in gLite 3.1 and gLite 3.2.

Plans:

Improved search/ dashboard for UMD usage.

Improved fields/search/dashboard for reporting including metrics.

Received Report on VOMS Core security assessment from UAB.

Note D4.4. took up a lot of the SVG chairs time.

1. Member, Observer, in Attendance [↑](#footnote-ref-1)
2. NEW, OPEN, CLOSED, REJECTED [↑](#footnote-ref-2)