EGI CSIRT team monthly meeting

Report of Contributions

Contribution ID: **0** Type: **not specified**

Group activities update and forward planning

Thursday, 18 November 2010 14:45 (15 minutes)

Update from group coordinators:

–IRTF (Leif)
Last month activites update
Wiki page update: https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting
update incident handling flowchart?
Critical Vulnerability handling procedure (Linda's draft)?
Plan for the coming month and quarter?

–Security monitoring (Daniel)
Last month activities update
Pakiti development
Nagios development
Security dashboard and integration
Plan for the coming month and quarter?

–Security drill (Sven)
Last month activites update
preparation for SSC4 NGI run - Spanish NGI
Plan for the coming month and quarter?

–Security training & dissemination (Dorine)
Last month activities update
https://wiki.egi.eu/csirt/index.php/Development_area_for_the_security_dissemination_website
Plan for the coming month and quarter?

Contribution ID: **1** Type: **not specified**

Minutes taker and Project update

Thursday, 18 November 2010 14:30 (5 minutes)

Minutes taker - DC of the week or the backup
Please add upload minutes to: https://wiki.egi.eu/csirt/index.php/EGI_CSIRT_monthly_meeting#Monthly_Meeting_Minute

Contribution ID: **2** Type: **not specified**

update from team members

Thursday, 18 November 2010 15:20 (5 minutes)

A quick roundtable update

Contribution ID: **3** Type: **not specified**

RTIR Discussion (Carlos and all)

Thursday, 18 November 2010 15:00 (20 minutes)

- Negotiation with egi it-support
- RTIR setup/installation package for egi it-support
- RTIR extensions/development works and possible timeline
- security officers information from GOCDB
- fine-grain access control (EGI SSO) for CSIRT, NGI security officers, site security officers etc.
- Pakiti/Nagios intergration
- Security dashboard/operation dashboard integration
- RTIR email templates

Contribution ID: **4** Type: **not specified**

Action review and AOB

Thursday, 18 November 2010 15:25 (5 minutes)

To review any pending actions and ongoing issues
https://rt.egi.eu/rt/index.html
A list of new actions from this meeting

AOB
Next monthly meeting: 21-Dec-2010?

Contribution ID: **5** Type: **not specified**

CSIRT and SVG Vulnerability assessment

Thursday, 18 November 2010 14:35 (5 minutes)

Copy of Linda's most recent email:

Definitions:

SLA software - Software distributed by EGI UMD (gLite, Unicore etc from EMI), IGE, or any software for which there is (or planned to be) SLA between provider and EGI.

Operating system software - Software that is part of the operating system (e.g. SL) or distributed with the operating system. (e.g.
openssl)

EGI Non SLA software - e.g. VO software etc.

Other Software - Software deployed in EGI which comes from elsewhere.
(Unlikely to be much from discussions with software providers)

Situations:

Incidents: ** Clearly CSIRT ** although SVG may get involved if they are due to exploiting software vulnerabilities.

Vulnerable systems due to:

Operational mis-configuration of sites (i.e. NOT due to e.g. scripts in gLite configuration which are software vulnerabilities) ** Clearly CSIRT **

Sites not updating their software to incorporate available patches ** Clearly CSIRT **

Vulnerabilities in operating systems - where patch is made available prior to announcing publicly:
CSIRT may enter in report-vulnerability and asks for risk assessment if they wish.
Always/if needed/not SVG task/only if potentially critical?
CSIRT ensures sites up to date. ** CSIRT/SVG - needs discussion **

Vulnerabilities in operating systems - BEFORE patch available (whether found by EGI members, reported to report-vulnerability, or announced publicly).
Entered in report-vulnerability.
CSIRT added to request
Risk Assessed using SVG criteria. (public raises risk usually) Target Date set as for other SVG issues.
CSIRT members (or RAT members who are also in CSIRT) chase operating system providers for fix.
** CSIRT/SVG -needs discussion **

Vulnerabilities in SLA software:
Clear that SVG issue handling process followed.
If made public, CSIRT also added to request (hopefully rare) ** Clearly SVG **

EGI Non SLA software - same as SLA software.

Other software - same as operating system software.

In all cases - if critical, critical issue handling process is invoked.
(I hope to work on it again today.) ** SVG/CSIRT collaboration for SLA Software, probably for all software **

Once a risk category is set, and the patch is available, and advisory distributed, then a vulnerability is no longer an SVG task - it becomes CSIRT to ensure sites patch.

Option 1: all vulnerabilities including OS vulnerabilities are assessed and tracked by EGI SVG; But for OS vulnerabilities CSIRT free to do anything they choose operationally, and override RAT's opinion on Risk if they choose.
If critical - move to critical vulnerability handling process.

Options 2: OS vulnerability, initial assessment is doen by EGI CSIRT: if it is time critical then it will be handled as a ad-hoc manner by EGI CSIRT, non-time critical will report to SVG and follow the SVG risk assessment procedure