Security Communication Endpoints

Maintaining GOC-DB information / Site Suspension and Re-certification

Sven Gabriel

Security Endpoints Communicatio

Problem: Out dated (security) contact information?

- Contact Information is entered in GOC-DB upon NGI/Site Registration/Certification
- Is it ever tested? Usually when we have to handle a new CRITICAL CVE, got a bit quiet this year.
- EGI-CSIRT experienced that not all contact information is maintained in GOC-DB
- Security communication is mostly only from EGI-CSIRT to NGIs/Sites, requesting an action.
- Security communications are less frequent/use other endpoints then operational communications.
- When contacting sites on security issues, usually time matters, solving communication endpoint issues then should be avoided.

Security Endpoints Communicatio

Suggestion: Frequent (bi-annual) Communication challenges **NGIs**

- Communication Method: RT-IR / mail
- Issue: mail contained a link to the RT-IR ticket, which is not accessible to recipients, solved, link removed.
- Challenge: RT-IR fetches NGI security contact info from GOC-DB automatically, (implemented in SSC framework, will be implemented in Operations RT-IR in January)
- EGI-CSIRT will open a ticket in RT-IR for every NGI (security contact), requesting an acknowledgement.
- When this is received, ticket will be closed.
- If no acknowledgement is received, Operations should contact NGI Management requesting an update of the respective information in GOC-DB.

Security Endpoints Communicatio

Suggestion: Frequent (bi-annual) Communication challenges **Sites**

- NGIs should make sure that contact information within NGIs are maintained as well
- NGIs are involved in the site certification procedure and should make sure that the security contact information is valid.
- NGIs should run a similar communication challenge against their sites at the same frequency (bi-annual)
- Can be combined with the NGI challenge by EGI-CSIRT asking the NGI-Security contact if the GOC-DB information for the sites is still up-to-date.

Suspending / re-certification RO-07-NIPNE

- Reason for suspension
  - Different WN appeared in CRITICAL vulnerability monitoring.
  - Contact info to ngi/site security contacts unclear in goc-db
  - Site did not reply to EGI-CSIRT tickets.
- Suspended on 05/12/13
- Re-Certification started 05/12/13
- EGI-CSIRT part of PROC09 re-certification finished 05/12/13
- RE-Certified 07/12/13
- Issues: Site wide pakiti monitoring showed some problems, these are solved