EGI-CSIRT – Operational Security

Activity Update

EGI-CSIRT

sveng@nikhef.nl, Nikhef, EGI-CSIRT

Activity Update / Overview

- Cloud Security
  - FedCloud EGI-CSIRT / Fedcloud F2F Jan 15 / Work packages defined
  - EGI Conf Lisbon Session: Security for cloud federations 20 May 2015 13:30
    - VM and User Management in Incident Response
    - Security Challenges for Cloud Environments
    - Security Challenges a Cloud Providers View

Security Operations: Incidents / Alerts, Advisories 26. Mar. 2015 – 30. Apr.

- No new incidents reported
  - 7 Vulnerability reports: Critical (1) / High (1) / Low (3), 2 Pending potentially critical (see next slide)
  - 2 Alerts/Advisories

A software product consuming a lot CSIRT cycles: perfSONAR

- Currently: Potential remote root exploit
  https://rt.egi.eu/rt/Ticket/Display.html?id=8479
- Monitoring (provided by perfsonar experts) of the possibly vulnerable instances/configurations is tedious.

Issues handled in perfSONAR

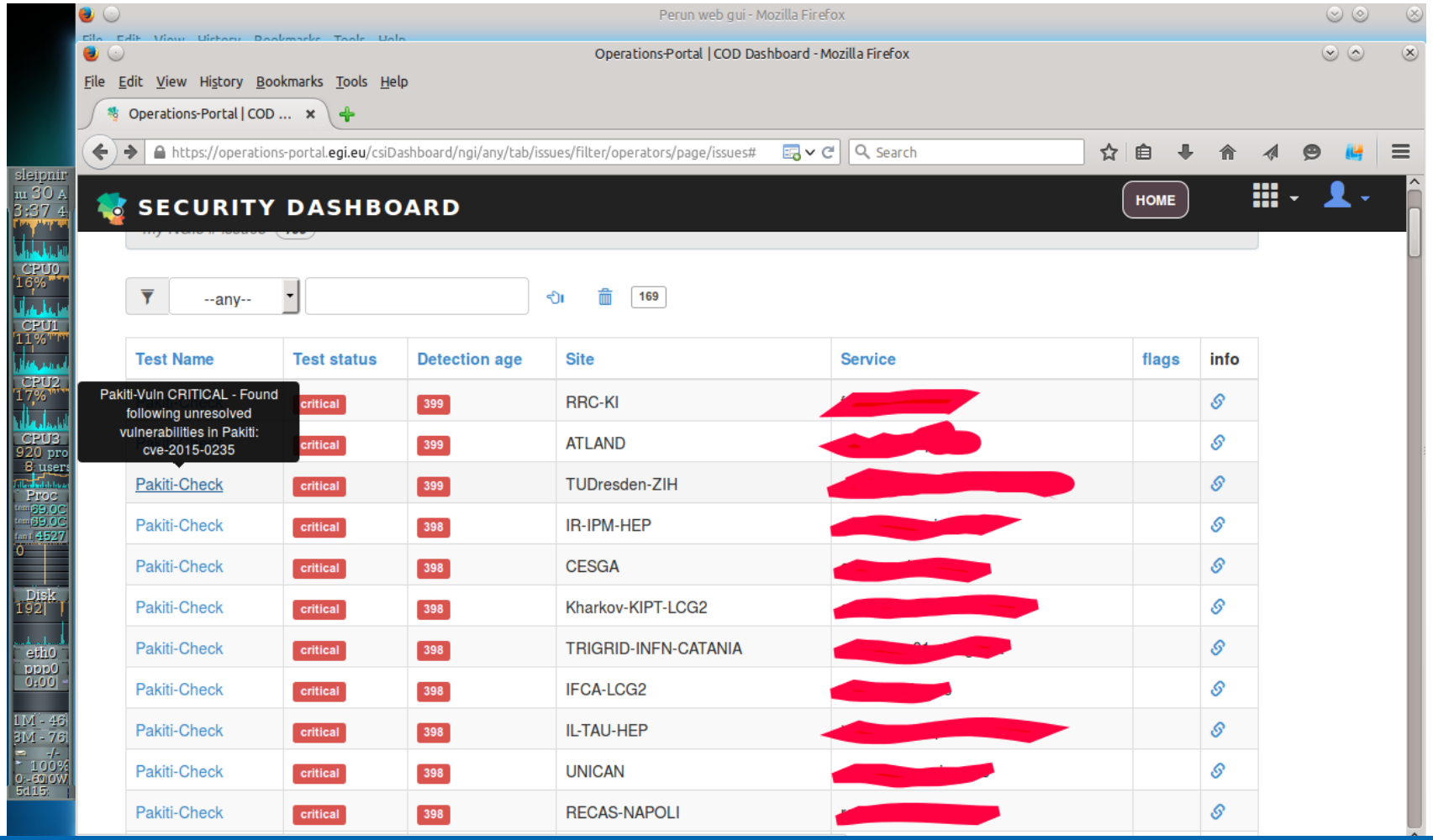
- Cacti graphs allows guests to change settings https://rt.egi.eu/guest/Ticket/Display.html?id=7162 June 2014 (Exploited)
- Perfsonar web interface problems https://rt.egi.eu/rt/Ticket/Display.html?id=6052 August 2014
- Installation without warning - https://rt.egi.eu/rt/Ticket/Display.html?id=7554 October 2014
- Incidents exploiting shellshock vulnerability within perfSONAR
- ex: *The NDGF-T1 Perfsonar server lla-ps.sunet.se was found to be compromised through shellshock on September 29. ... + 3 more*

Security Operations: CRITICAL CVE handling

- CVE-2014-9322/CVE-2014-6271/6277/CVE-2015-1815/CVE-2010-3081/CVE-2013-2094: 16 Sites / 1 site suspended
- Re-Certification: 4 Sites **DONE**.
- It should not be possible for RODs to silently re-certify Sites / No Control hook in this process. Can we get a control hook in this process? **update?**
- Example: BG05, suspended by EGI-CSIRT (20-Apr-2015 12.39.28), got silently re-certified by ROD (22-Apr-2015 12.58.12)
- Action Point? Who?

Nagios / Security Dashboard / false positives, **Update from Nagios team?**

https://ggus.eu/index.php?mode=ticket_info&ticket_id=112096



Critical Vulnerability Handling Procedure recap from OMB 26. Mar

- Security Monitoring jobs are regular grid jobs, no way to send it to a particular WN
- Current procedure handling critical CVEs is:
- EGI-CSIRT opens ticket in RT-IR when a host is found vulnerable for a CRITICAL CVEs
- No way to probe the host again from external / Host disappears from Monitoring
- Solution: Site runs pakiti client manually, monitoring data gets updated.
- This step needs to be a requirement in the CRITICAL CVE handling procedure

Critical Vulnerability Handling Procedure update from OMB 26. Mar

- Feedback received from NGI UK
- Issues with pakiti client deployment as tarball, **DONE** now a rpm in epel
- Instructions updated on: https://wiki.egi.eu/csirt/index.php/Pakiti_client
- Feedback from NGI-CH: Automated Notification of Site-Security contacts
- A reasonable solution (reporting from Nagios) will take some time. From Pakiti we could enable sending mail in the same way what we do at the moment for EGI CSIRT. It doesn't take into account possible mitigations.
- No further feedback received, we assume we can change the procedure accordingly.

Self Assessment of the NGI/Site Security Teams

- EGI-CSIRT got reviewed by TI and certified according to maturity parameters
- The same parameters are used for an interactive self assessment https://check.ncsc.nl/questionnaire/
- To get an overview about the security teams in EGI it would help to find order 10 sites to do the self assessment

Self Assessment of the NGI/Site Security Teams

https://check.ncsc.nl/questionnaire/

Search

GCCS 2015 The Netherlands

GCCS CSIRT MATURITY QUICK SCAN

Measurement. Progress. Security.

HOME
START QUICK SCAN
BROCHURE
CSIRT MATURITY KIT
GCCS 2015
ABOUT / CONTACT

MATURITY QUICK SCAN QUESTIONNAIRE

General details

What is the name of your organisation	
How many people work on the CSIRT team? (including part-time)	○ No formal team assigned ○ One, maybe two ○ 3 to 4 ○ 5 to 8 ○ more than 8
How long does your CSIRT formally exist?	○ It has not started yet ○ It has not been formalised yet ○ 0 to 3 years