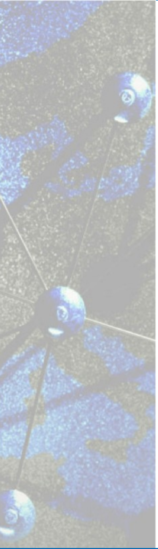


Security in EGI FedCloud

Incident Response / Security Challenges

Sven Gabriel, sveng@nikhef.nl

Nikhef http://nikhef.nl

EGI-CSIRT https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page

Incident Response in EGI

Incident Response in EGI

Incident Response in EGI

Impossible task:

- 54 different jurisdictions
- Sites are independent – very little centralized power
- Sites range from big national facilities to small underfunded departmental systems.
- Sites are usually already in the constituency of some other CSIRT.

How do you deal with this?

Incident Response in EGI

Impossible task:

- 54 different jurisdictions
- Sites are independent – very little centralized power
- Sites range from big national facilities to small underfunded departmental systems.
- Sites are usually already in the constituency of some other CSIRT.

How do you deal with this? You need to be:

- pragmatic
- humble
- and good at social engineering.

Incident Response in EGI

Basically, EGI is a federation of National Grid Infrastructures (NGIs) – typically one per country – that each encompass something between 1 and 40 physical sites.

Incident Response in EGI

- High level policies give a framework to operate in.
- Last resort – suspension. Follow the rules, or you can’t be in our club.

Incident Response in EGI

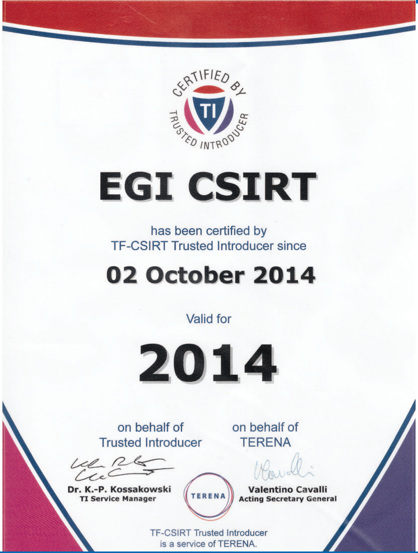
- Each NGI has an appointed NGI security officer.
- A core subset (about a dozen) of the NGI security officers form the EGI Incident Response Task Force (IRTF).
- Have a grid / systems background
- **We need a FedCloud tech expert in IRTF**

Incident Response in EGI

IRTF members serve as EGI Security Officer on duty, on a weekly rota.

- Handle incident reports
- Keep an eye on monitoring
- Keep things falling between chairs
- Have signed a CodeOfConduct

Incident Response in EGI



CERTIFIED BY TI TRUSTED INTRODUCER

EGI CSIRT

has been certified by
TF-CSIRT Trusted Introducer since

02 October 2014

Valid for

2014

on behalf of Trusted Introducer	on behalf of TERENA
Dr. K.-P. Kossakowski **TI Service Manager**	**Valentino Cavalli** **Acting Secretary General**

TERENA

TF-CSIRT Trusted Introducer
is a service of TERENA.

- candidate (12)
- listed (119) (2009)
- accredited (97) (2012)
- certified (8) (2014)

Incident Response in EGI

How to monitor the security status of the distributed sites?

Realization: we have an infrastructure to run computation jobs!
Use that also for monitoring.

Incident Response in EGI

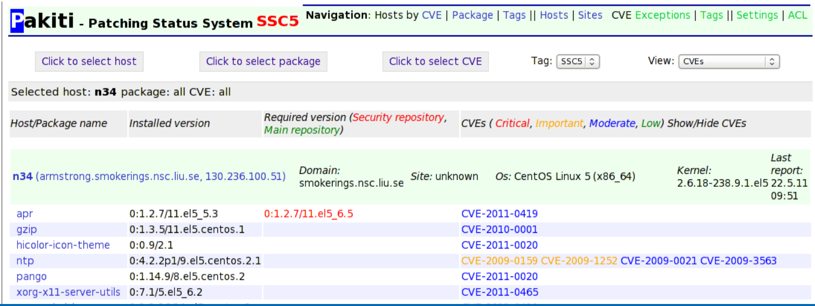
Nagios

- Monitoring jobs submit passive probe data into Nagios.
- Checks e.g. bad file permissions, vulnerable kernel modules.
- Used to quickly run custom tests across sites, e.g. to monitor CVE-2009-4033 which caused /var/log/acpid to be created with random permissions.

Incident Response in EGI

Pakiti

- Daily jobs dump the RPM data base and cross-checks against OVAL data.
- Web interface for monitoring, e-mail alerts for critical vulns.
- *Very* useful, but only gives results for a sample of the compute nodes at a site.



Pakiti - Patching Status System SSC5

Navigation: Hosts by CVE | Package | Tags || Hosts | Sites CVE Exceptions | Tags || Settings | ACL
Click to select host
Click to select package
Click to select CVE
Tag: SSC5
View: CVEs

Selected host: **n34** package: all CVE: all

Host/Package name	*Installed version*	*Required version (Security repository, Main repository)*	*CVEs (Critical, Important, Moderate, Low) Show/Hide CVEs*
n34 (armstrong.smokerings.nsc.liu.se, 130.236.100.51)	*Domain:* smokerings.nsc.liu.se	*Site:* unknown *Os:* CentOS Linux 5 (x86_64)	*Kernel:* 2.6.18-238.9.1.el5 *Last report:* 22.5.11 09:51
apr	0:1.2.7/11.el5_5.3	0:1.2.7/11.el5_6.5	CVE-2011-0419
gzip	0:1.3.5/11.el5.centos.1		CVE-2010-0001
hicolor-icon-theme	0:0.9/2.1		CVE-2011-0020
ntp	0:4.2.2p1/9.el5.centos.2.1		CVE-2009-0159 CVE-2009-1252 CVE-2009-0021 CVE-2009-3563
pango	0:1.14.9/8.el5.centos.2		CVE-2011-0020
xorg-x11-server-utils	0:7.1/5.el5_6.2		CVE-2011-0465

Incident Response in EGI

Security Dashboard

Monitoring data from Nagios and Pakiti are aggregated and presented in the Security Dashboard area of the Operations Portal.

Incident Response in EGI

- What happens when we get an incident?
- What *is* an incident?

Incident Response in EGI

- What happens when we get an incident?
- What *is* an incident?

An [grid] incident is any real or suspected event that poses a real or potential threat to the integrity of [grid] services, resources, infrastructure, or identities.

Anything can be labeled a grid security incident if you feel like it! (This is where you need to be pragmatic. . .)

Incident Response in EGI

The EGI incident response procedure is brief, but establishes a flat structure with maximum info sharing.

(This is where social engineering comes in; it turns out professionally run CSIRTs have all sorts of privacy and disclosure policies that can hinder the information flow. You need to be able to bypass that in clever ways[1].)

[1] Preferably without making lots of enemies

Incident Response in EGI

Each incident is assigned an IRTF member as incident coordinator, who

- issues a heads-up warning to all sites
- works with the victim site to investigate the incident, possibly issuing additional all-sites broadcasts as new information is discovered
- coordinates the incident with other players (VOs, CAs, other CSIRTs, law enforcement. . .)
- makes sure a closure report is sent to all sites

Incident Response in EGI

Incident Response Prodedure:
`https://documents.egi.eu/public/RetrieveFile?docid=47`

- communication templates
- target times / what to investigate
- forensics

Incident Response in EGI

Total number of incidents involving grid technology:

Incident Response in EGI

Total number of incidents involving grid technology: 1

Incident Response in EGI

EGI-20110418-01	stolen ssh credentials
EGI-20110301-01	bruteforce ssh
EGI-20110121	web server misconfig
EGI-20111201-01	bruteforce ssh
EGI-20101018-01	bruteforce ssh
EGI-20100929-01	stolen ssh credentials
EGI-20100722	bruteforce ssh
EGI-20100707-01	stolen ssh credentials/remote vulns in CMSes
EGEE-20091204	stolen ssh credentials/X keyboard sniffing
GRID-SEC-001	stolen ssh credentials

Incident Response in EGI

- Large majority of incidents due to stolen or weak ssh credentials
- We have no power to force sites to deploy e.g. two factor auth
- We do try to motivate sites to install important security patches, partly to offset the potential damage from user level intrusions
- **CMF are juicy targets**

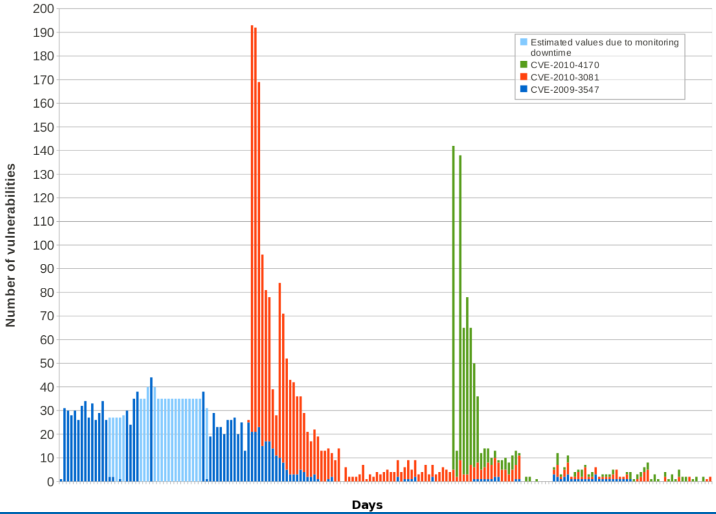
Incident Response in EGI

- Security Intelligence Group (SIG) monitors public and non-public sources for new vulns
- The Risk Assessment Team determines how serious new vulns are
- The EGI CSIRT produces detailed advisories that are broadcast to sites

Incident Response in EGI

- When new serious vulns appeared we used to issue an advisory, watch Pakiti for a while to make sure sites applied patches, and then forget about it.
- This didn't work; new vulnerable nodes keep appearing – bad config management, nodes that were under maintenance when patches were applied. . .
- We now continuously monitor for vulnerable nodes and slap them down as they appear.

Incident Response in EGI



Incident Response in EGI

What to expect (Stats from Okeanos):

- Users: 7000+ registered
- Clusters 13
- Nodes 171
- VM Instances 5074
- Virtual CPUs 11027
- Physical CPUs 4136

Incidents per year:

- 87 - Low Severity
- 330 - Medium Severity
- 94 - High Severity

Incident Response in EGI

Discussion: Important for efficient IR in FedCloud

- Centrally Suspend User DNs (See http://wiki.nikhef.nl/grid/Argus_Global_Banning_Setup_Overview
- Extend Central User Suspension concept to the suspension of VMs
- Is this possible? what would be needed (development)? Who can do this?

Incident Response in EGI

Finally, we try to be good community members and maintain good relations with neighbouring CSIRTs at all levels.

Want to report an incident, ... send a mail to **abuse .at. egi.eu**

Incident Response in EGI

Security Service Challenges