UKRI Science and Technology Facilities Council

IRIS Security Workshop

David Crooks
on behalf of the IRIS Security Team

david.crooks@stfc.ac.uk
Team: security@iris.ac.uk

iris
EGI CSIRT

Overview

- This workshop is the continuation of a long history of security workshops held at HEPSYSMAN meetings
- Held almost every year around June, typically one day meeting
  - Forensics training, topics of special interest
- Last year, spent the morning on procedures and the afternoon on digital forensics
- This year, spread workshops throughout the year via Zoom

Logistics

- Aim to have a 15-20 minute break around 3.20pm, and finish by 5pm
- Ideally keep cameras on while participating in discussion, but as you like
- We will not be recording this session: identify some note takers
- Not anticipating particularly sensitive discussions
  - but this is a security meeting so treat information appropriately
- Any issues please use the chat, either to everyone or me privately

Plan for today

- Before coffee

- Look at operational security structures for GridPP and IRIS
  - Some material GridPP specific, but consider what we need for IRIS
- Discuss security procedures at our sites/facilities

- Continuous process – plan to do this yearly
  - Both opportunity to discuss, and build plans for the future

Plan for today

- After coffee

- Operational security tools
  - What do people use?
  - What would people like to use?
  - How can the team help?

- Topics for the future

EGI CSIRT + SVG

- Specifically applicable to GridPP
  - For IRIS, overlap via IRIS Security Team
- EGI CSIRT
  - Incident Response
  - Monitoring
  - Drills
  - Training
- EGI SVG: Software Vulnerability Group

Incident response

- Incident response for GridPP ultimately coordinated by EGI CSIRT Incident Response Task Force (IRTF)
- IRTF on duty rota currently comprises NGI Security Officers for
    - CERN
    - NGI_NL
    - NGI_CZ
    - NGI_SI
    - NGI_IBERGRID
    - NGI_UK

IRTF: Roles and responsibilities

- Incident coordination
- Critical vulnerability tracking
  - On duty officer raises a ticket, followed up by EGI Ops
- Communication Challenges
- Service Security Challenges
- Liaison with other CSIRTs

IRTF: Monitoring

- Security dashboard
  - https://operations-portal.egi.eu
- Combines results from pakiti (sites should see their own results)
  - https://pakiti.egi.eu
- and secmon (accessible by NGI security officers)
  - Checks possible mitigations
- Pakiti gives patch status
- Secmon uses Nagios to check for mitigations (ARGO)
  - Combined result means pakiti is not the whole story

Purpose of the EGI Software Vulnerability Group (SVG)

- "To minimize the risk to the infrastructure arising from software vulnerabilities”

- **To Prevent Security Incidents**

- SVG has been handling software vulnerabilities in EGI and its predecessors for more than a decade.
- Started with Grid Middleware – as no-one was handling these, then evolved to handle any vulnerabilities relevant to the EGI distributed infrastructure

EGI SVG basic procedure

- Anyone may report a vulnerability to report-vulnerability@egi.eu
- If it has not been announced as fixed by the provider, SVG contacts the software provider
- If relevant to EGI the risk in the EGI environment is assessed, and put in 1 of 4 categories – ‘Critical’, ‘High’, ‘Moderate’ or ‘Low’
- If it has not been fixed, Target Date (TD) for resolution is set - ‘High’ 6 weeks, ‘Moderate’ 4 months, ‘Low’ 1 year

EGI SVG basic procedure

- Advisory is issued by SVG
  - If the issue is ‘Critical’ or ‘High’ in the EGI infrastructure
  - When the vulnerability is fixed if EGI SVG is the main handler of vulnerabilities for this software, or software is in EGI Repository regardless of the risk.
  - If we think there is a good reason to issue an advisory to the sites
- Priority given to Critical vulnerabilities – handle within 1 day

Now increased scope and evolving procedure

- The EOSC catalogue is a catalogue of services available to researchers
  - https://marketplace.eosc-portal.eu/
- Scope is now evolving to include the EOSC hub Portfolio
  - Common services like accounting, AAI, Marketplace software itself
  - But NOT the 100s of other service in the catalogue
- Procedure changing due to the increased inhomogeneity of services and proliferation of software and services as well as increased scope
- Setting up ‘Deployment Expert Group’ to cope with this

Deployment Expert Group (DEG)

- SVG members cannot be expert in all software and services
  - Need to call on others who select, configure, and deploy services
- Deployment expert group’s job is to:--
  - Look out for vulnerabilities in software they deploy and report them
  - Respond when asked ‘Is this software in scope? Do you use it?
  - Volunteer to help investigate and risk assess a vulnerability when they have expertise
- Scope will also depend on participation in the DEG.

EGI CSIRT/SVG + IRIS

- EGI Broadcasts are sent during incidents and with advisories about vulnerabilities
- Agreement with EGI CSIRT to share incident indicators with IRIS Security Team
  - Lets us check for impact across IRIS
  - Also share back from IRIS to EGI CSIRT to support global incident response
- Can also pass on vulnerabilities
  - May not always have same impact for all IRIS sites

IRIS Security Team: security@iris.ac.uk

- Builds from existing team supporting operational security in GridPP and helping coordinate incident response for the UK for incidents coordinated by EGI CSIRT
- Now contains representatives from Grid/HPC/Cloud across IRIS
  - At least two from each by design
  - CSIRT Code of Practice to affirm acceptance of TLP labels
- Primary role is to coordinate incident response and share security information across IRIS
  - Already discussed setting up secure channels, in progress
  - Coordinate with other CSIRTs, particularly (inter)national Janet CSIRT and EGI CSIRT

IRIS Security Team: security@iris.ac.uk

- Current and future work
  - Training events
  - Security challenges: communications, traceability and service challenges are possible
    - Start with communications challenge in due course

- What can the team, being distributed, do to help secure IRIS?
  - Monitoring
  - Tools
  - (all backed by IRIS-IAM)

Before coffee

Before coffee

- Talk about procedures
- Service providers should know what to do in case of a security incident
- Opportunity to discuss what we have in place + and what we need
- If we come out of this with sites having some action items, that’s great!

- Also explore what we specifically need in IRIS as we grow our capability
  - Already talking about secure channels
  - What about vulnerability assessments?

Before coffee: mini tabletop

- One of the central security teams reports unusual network traffic to you.

  - What do you do?
  - Who do you talk to?
  - Do you have a plan in place?

- Discuss!

After coffee

After coffee: Operational Security Tools

- Time for a poll!
- Yes: this is a security officer asking you to enter a link ☺
- http://etc.ch/DGhX

After coffee: Operational Security Tools

- Ongoing discussion (held over from last Security Workshop)
- What tools should sites have in place?
  - Network tools
  - Scanning
  - Host based tools
  - Central logging
  - Threat intelligence (threat feeds/systems that monitor your traffic)
- Other operational security topics for today

Topics for next workshop

- Options for next time
- Follow-up/more detail from today
- Forensics
- Tabletop exercise