GridPP Security Update

Matt, for the Security Team

GridPP51, 27th March 2024

Most importantly…

There have been no critical incidents involving our sites.

Team structure, Contact Info

- No changes.
  - The GridPP "portion" of the IRIS security team provides the duty rota.
  - Meet fortnightly along with members from DiRAC, Cloud, HPC.
- security@iris.ac.uk is our contact address.
- abuse@egi.eu is the address for incidents (cc in us)
- security-discussion is the list that should be used for sensitive discussion between sites.
  - TB-SUPPORT is publicly archived – although we can excise material posted here by accident.
- Moved to confluence for our documentation.
- Members on the EGI-CSIRT and the Software Vulnerability Group.
- New faces within "adjacent" teams within the UKRI and STFC

Communications

- E-mail doesn't feel as reliable as it used to be.
- Blocked emails, list solutions not talking to each other, some sites being forced to use personal emails rather than a generic.
- And there's always just details going out of date.
- As an aside, we've never settled on a method of signing or encrypting emails (and maybe never will).
- No panacea for this
  - Comms challenges can help, but there's no perfect system to conduct these and they're not "free to run" - they take effort.
  - If in doubt that an email got through it's good to ask
    - Sometimes people are just busy too!

Landscape

- The threat level is "consistently elevated"
  - "Bad actors" have a breadth of motivations and capabilities.
  - The age of the "script kiddie" feels long past.
    - I'm pretty sure they're still out there though.
- Increase of "institutional awareness" of security issues.
  - Generally this is a positive thing.
  - Risk of mandates being overly broad and not meeting the needs of research.
    - …safelinks
    - This is always somewhat of a balancing act.

CentOS is dead! Long Live…

- CentOS7 updates are few and far between, and have been for a while.
  - EL7 EOL June 30th
  - Speculation: the last 12 months don't bode well for when EL8/9 start to near EOL.
  - Within the UK no clear contender between Rocky and Alma
    - CERN went with Alma, although a number of UK sites have gone for Rocky.
    - Circumstances have also pushed some sites towards EL8 rather than 9.
    - No one laughs anymore if you mention the idea of moving to Debian.
  - The outcome of this is that we've possibly never had a more diverse range of operating systems on UK infrastructure.
    - And Rocky and Alma could drift further apart.
- Need to take (and keep) stock of the situation.

Taking Stock

- It looks to be a growing need for us to take a "census" of sites.
  - Different from the site survey.
- The gocdb is useful, but doesn't provide the whole picture.
  - OS choices.
  - Batch systems.
  - Virtualisation/Containerisation and/or Deployment technologies.
  - Local constraints
- This will help us focus efforts in areas such as the Software Vulnerability Group

Software Vulnerability Group

- Long standing leadership position in the SVG.
- Looking to evolve and redefine scope.
  - Subject to "availability of expertise" and effort.
- Membership does not grant omniscience
  - We encourage letting the SVG know if you ever spot something of interest.
- There's disheartening common threads among many of the vulnerabilities
  - Netfilter, use-after-free, disable network namespaces.

Purpose of the EGI Software Vulnerability Group

To minimize the risk of security incidents due to software vulnerabilities.

Numbers Since 1st September 2023

- 27 Vulnerabilities reported
- 14 Advisories sent
  - 3 ‘Critical’ risk
  - 10 ‘High’ risk
  - 1 ‘Alert’

- Advisories when public are now placed on advisories.egi.eu

Other SVG

- We now have a new advisory style/template.
  - Been using this since September 2023 (Sites will probably have noticed.)
  - After lots of discussion, we agreed a new style template for the advisory.
  - This makes the advisories shorter and more focused on what sites need to do
  - People seem happy with it.
  - It also fits better with the markdown, which makes making public on advisories.egi.eu better
    - Including functional links
- Planning on further evolution
  - Scope depending on participation
  - Improved more formalized sharing of information, beyond EGI (including GridPP) and a few others we currently share with - including with other UK people

Information Sharing

- There have been increased efforts to set up communication channels for intelligence sharing.
  - Starting with simple, routine forwarding of information such as vulnerability advisories.
    - Also gels with the SOC work with tools such as MISP.
  - Building community, trust and encouraging reciprocation.
  - All sides of these exchanges need to have an understanding of the spirit and conditions of the information being shared, for example with the TLP protocol.

SOC

- Strong UK involvement in the Security Operation Centre WG.
  - Another Hackathon just last week.
  - David will explain more.
  - Zeek, MISP and pDNSSOC
- Growing SOC presence at institutes
  - For certain values of "SOC"
  - Need to make sure we're all on the same page.

Tokens and AAI

- A lot of UK involvement on this front.
  - WLCG AuthZ group
  - WISE, EUGridPMA
  - Token Trust and Traceability (TTT) and Grand Unified Token (GUT) working groups
  - TIIME Unconference in February.
- A lot of practical efforts in this area too
  - IRIS IAM
  - See DIRAC token work
  - General good level of "token enabling" across GridPP resources.

TTT

- The TTT WG meets ~monthly.
  - Our first target is the documentation – you can't trust what you don't know.
    - Explain (and understand ourselves) the paradigm shift
    - User and Admin side
    - Make sure admins are equipped to "self-test" using the dteam VO.
    - Check how current banning mechanisms work in a token regime (they probably don't).
    - Set up procedures (and expectations) for contacting Issuers, and for token infrastructure changes (like the recent change of Issuer details for WLCG VOs).
  - Working with the GUT WG to "bake in" Trust.
- Happy to have any more inputs (or at least test drivers for our docs once they're done.

Documentation and Training

- Something from last year's Site Security Survey was a desire for documentation.
  - Even White Papers.
- This was heard, but good documentation takes time.
- Confluence provides a good location to share potentially sensitive information.
- A good first step would be to provide pointers to the wealth of information out there.
  - A "Quiet Friday Afternoon" job.
- Considering forum and location to run F2F training.

Cyber Assessment Framework

- https://www.ncsc.gov.uk/collection/caf
- Completed for the Tier 1
  - Was an extensive project, many person-hours.
  - Experience that could be shared.
- Assessment processes (Risk and Otherwise) are a useful process.
  - Not just a box ticking exercise.
  - And becoming necessary/mandatory – evidence of compliance to a recognised Assessment Framework/certification is becoming increasingly desired.
    - ISO27001, Cyber Essentials.
- CAF part of the IRIS Security Strategy.

Wrap Up

- Evolution on all sides of the Landscape.
  - Institutions
  - Organisations
  - Frameworks
  - Threats
  - Technology
- We need to evolve too.

Any Questions?