IRIS Security Update

December 2023, Leicester

Matt Doidge, on behalf of the IRIS Security Team
security@iris.ac.uk

Overview

- Landscape
- IRIS Security Status and Developments in 2023
- Vulnerabilities
- SSC
- GridPP Site Security Survey
- Schools and Hackathons

This will be mostly a look at what we've done over the last 11 months, David gives the forward look tomorrow.

Speaker Context

- I am a founding member of the IRIS Security Team and a long standing member of GridPP
  - Recently joined the EGI CSIRT, expanding the UK presence on the team and the UK contribution to the CSIRT duty rota.
  - Chair of the WLCG Token Trust and Traceability WG.
- This explains the framing of that presented here.
  - The content maybe a little GridPP/WLCG/EGI/CERN-centric
  - Much is still relevant to all.

The most important slide?

There were zero critical security incidents directly involving IRIS providers or members this year.

The Threat Landscape

- Threat Levels are still high.
  - This is the "new normal".
  - Bad actors operate widely, in a variety of guises (and sometimes causes).
    - Hacking is an industry.
    - The Geopolitical Situation hasn't calmed down either.
- Cyberattacks are regular headline news items, and affect us all.
  - Anyone with a USS pension will attest to this.
  - And hopefully no one is trying to complete on a house purchase right now.

The IRIS Security Team

- Consists of members from across the IRIS Providers (Grid, HPC, Cloud), led by David Crooks.
- The team is largely unchanged since January, except joined by Adrian from Cambridge in his cybersecurity role there.
- Meet fortnightly to discuss vulnerabilities, threats and plan.
  - In addition to internal comms within each group.
- "On Duty" Rota with a core from the grid team providing continuous business hours cover.
- Move to improve vulnerability information dissemination throughout the groups and communities.
  - This requires the development of procedures and policies to do so in a structured, routine fashion.

Communications

- The official way to contact the security team is via security@iris.ac.uk
- There is a security-discussion jiscmail, currently GridPP site centric.
  - It is a non-archived closed list
  - Thoughts on if we want a separate list for other groups.
- Working on the means and method for disseminating somewhat sensitive information among concerned parties (such as recently disclosed vulnerabilities).
- Looking at "on-prem" ticketing solutions.
- Confluence as a means of securely sharing sensitive information.

Themes from some of this year's vulnerabilities

- Reemergence (although they never really went away) of CPU vulnerabilities, affecting multiple vendors:
  - "Downfall"
  - "Zenbleed"
    - An extra dimension to these issues is to patch them out is often to "patch out" certain CPU efficiency features.
- Constant reminders to keep your BMCs away from the internet
- The Linux Kernel Netfilter keeps needing more patches then <insert pun here>

More Vulnerability Themes: S(OS).

- EL7 officially reaches EOL June 2024
  - But already has one foot in the grave.
  - Very slow to patch, or just won't for "moderate" issues.
- Recent business decisions by RH make life difficult for EL forks
  - This could eventual push away from EL within the communities that have historically relied to it (particularly PP).
  - A wider ecosystem could provide challenges for activities such as security monitoring and threat sharing.
    - But there are advantages to avoiding OS lock in.
- https://advisories.egi.eu/

EGI Security Service Challenge

- In March year, with the cooperation of the CMS WLCG VO, the EGI CSIRT ran a coordinated security exercise.
  - In essence simulating compromised credentials being used to build a "botnet" within the infrastructure.
  - Designed to test awareness, communication and readiness.
- There was an optional, bonus element for admins who wanted to perform forensic analysis on the rogue processes.
- Should be noted that there was a lot of effort required to set up and maintain the "attacking" infrastructure.
  - In addition analysing the results was perhaps an equal endeavour.
- Strong UK involvement in both the production and planning (particularly Katy from RAL as one of the CMS reps), and an excellent showing for those UK sites that took apart
- See the TechEx talk for a better writeup.

SOC WG Hackathon

- Hosted during a week this Summer, at Coseners.
- Very productive week, members from the UK were joined from colleagues from all over the world.
  - The locale is very conducive to such activities.
- Development activities included maturing pDNSSoc, MISP integration, and writing documentation.

- Also this summer Coseners hosted an IAM Hackathon arranged by Tom Dack, which was equally as productive.

SOCs, Threat Sharing, EDRs

- Strong UK Involvement in the development and deployment of Security Operation Centre solutions.
  - "Heavyweight": Involving deep packet inspection with Zeek, Elasticsearch.
  - "Lightweight": pDNSSoc - using passive DNS information.
- Patch status monitoring with pakiti.
- Threat Sharing with MISP.
  - Opens other uses of the Indicator of Compromise information.
  - Can be integrated into log analysis, other monitoring or protection.
- Spread of "Endpoint Detection and Response" deployments.
  - Need to understand the impact these will have on workloads.

Thematic CERN School of Computing on Security

- This year saw the second Security focused CERN School of Computing.
  - The third is planned for Autumn 2024.
- Another instance of strong UK involvement.
  - David Crooks is a member of the program committee and ran the SOC lectures and exercises.
  - Tom Dack has taken over teaching of the AAI portion.
  - Liam and James from STFC attended as Students.
- The material is highly transferable to IRIS contexts. A good basis for future trainings.
  - Formed the bones of the Workshop at the ROE in January.

GridPP Site Security Survey

- This spring the security team wrote and disseminated a site security survey to GridPP sites.
  - Asking questions about policies, procedures and protections.
  - Also asked what was wanted from the security team.
- Happy to report that there were no red flags.
  - The basics of central logging and strong firewalls were everywhere, and more controls besides.
  - Everyone took security seriously.
- Some meta-lessons learnt, about how to format a survey, and what are useful questions to ask.
- A summary of the results were presented at the GridPP meeting.

Site Security Survey Continued

- A common theme from the questions asking "what do you want from the security team" was more training and documentation.
  - From step-by-step instructions to follow to full white papers on best practice.
  - This gels well with the incident response best practice of "write everything down ahead of time".
- Would like to repeat the Survey for other IRIS providers, but first need a single point of truth for contacts.
  - For the grid this is the gocdb.
  - For IRIS this will be the (other) gocdb.

Summary

- A busy year, but for the right reasons.
  - Security Challenges, Surveys, Schools, Hackathons.
- There are many plans in the works.
  - SOCs, EDRs, Threat Intelligence, Vulnerability Sharing and Monitoring, Training.
- Although the first step is a simple one, we need to start with a reliable list of contacts and resources.