June 11th 2026
Thursday

OSG Security Team

Because you're tired of hearing about AI

= AI

OSG Security Team

Mark Krenz

Adrian Crenshaw

Megha Moncy

Vishal Singh Bhardvaj

(Team members from IU)

Responsibilities

Scanning for vulns

Finding vulnerabilities relevant to the OSG consortium

Weekly Nessus scanning of OSG-managed infrastructure

~180 hosts monitored

Coordination with service owners on remediation

Threat Intel

Monitoring emerging threats and security advisories

CVEs reviewed: 100+ per day

Deep-dive analysis: 150+ (2025), 170+ (2026 YTD)

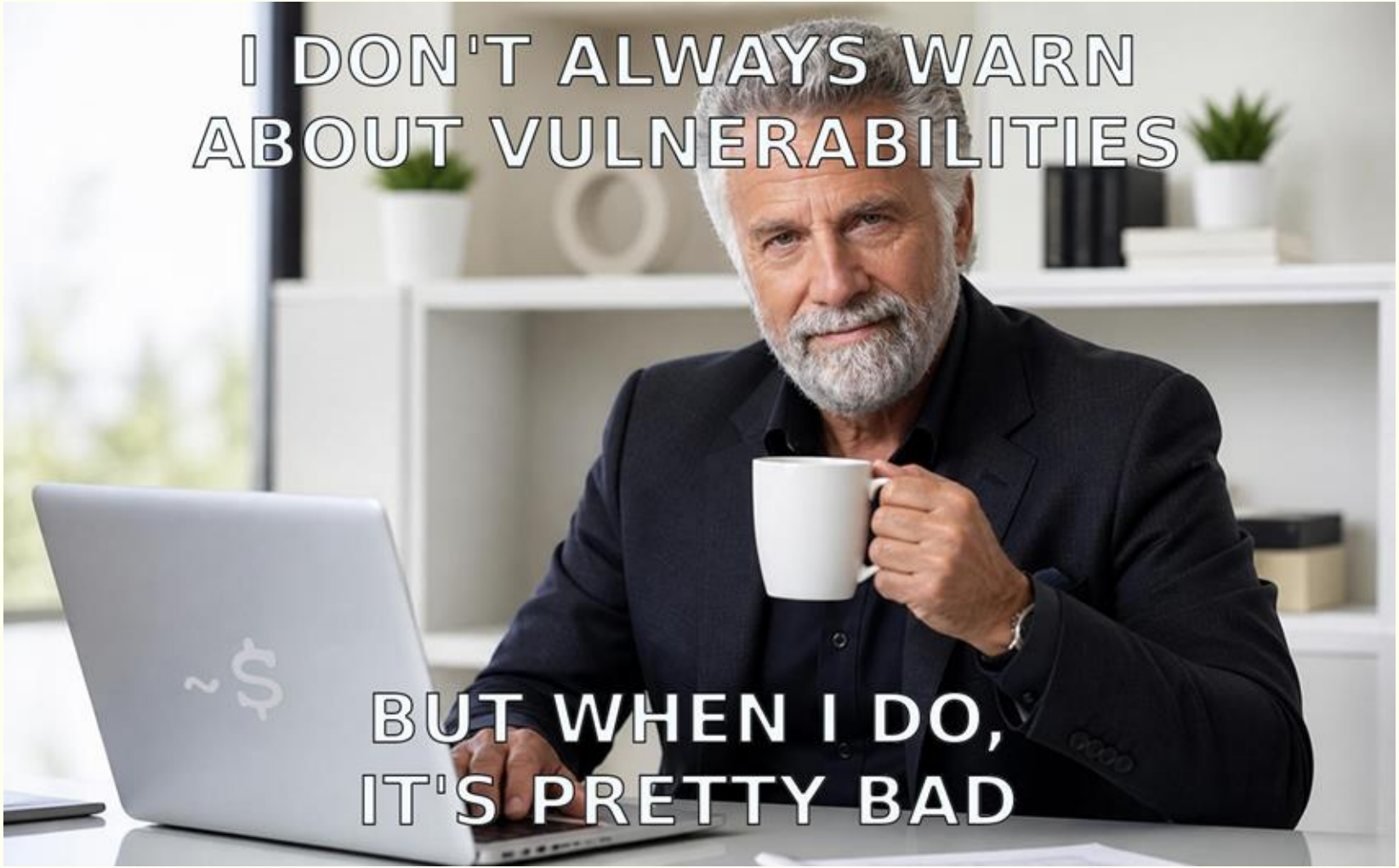
Communications sent: 22 (2025), 43 (2026 YTD)

Community

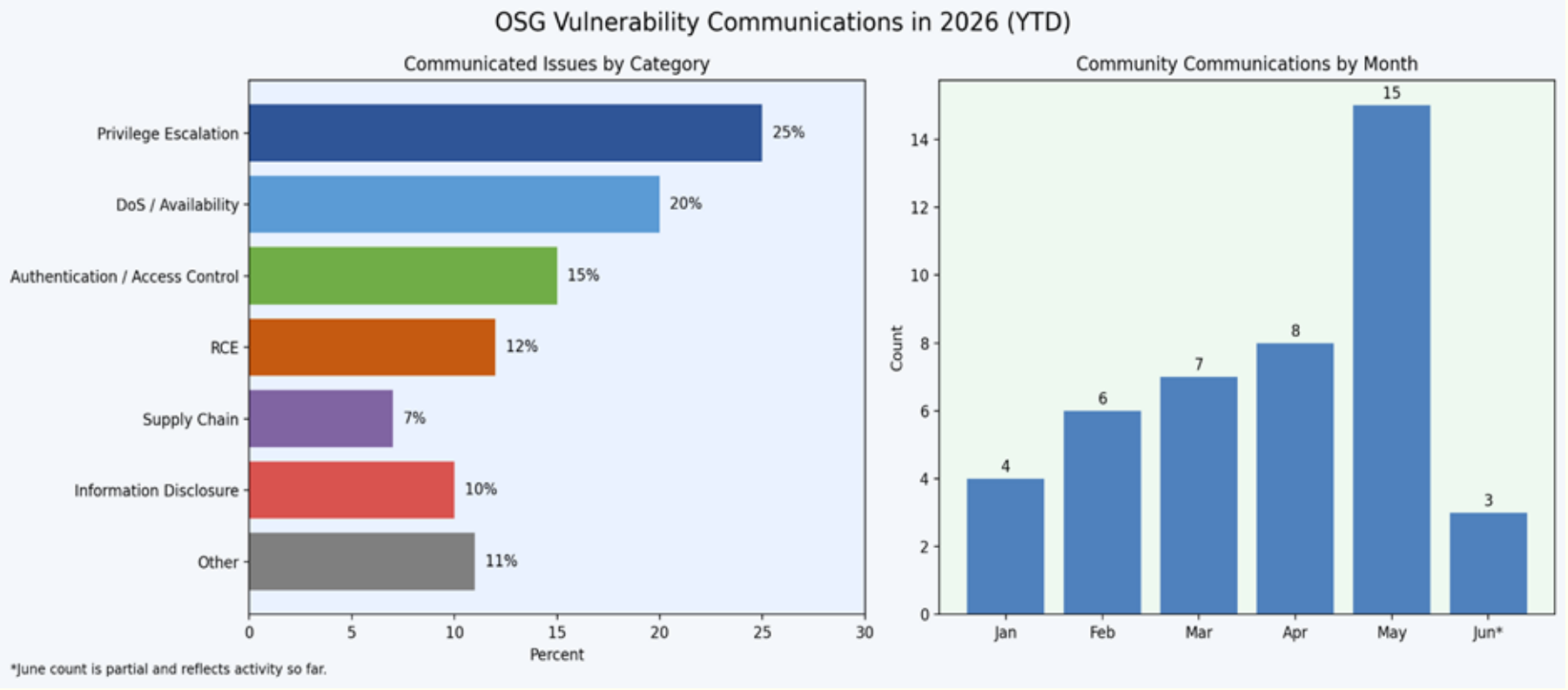
Supporting security discussions in Slack, Ops meetings,and PATh weekly meetings

Security coordination with HTCondor, Pelican, LHC, and community services

Helping teams understand risk and prioritize fixes


I DON'T ALWAYS WARN
ABOUT VULNERABILITIES
BUT WHEN I DO,
IT'S PRETTY BAD

Threat Intelligence Communication

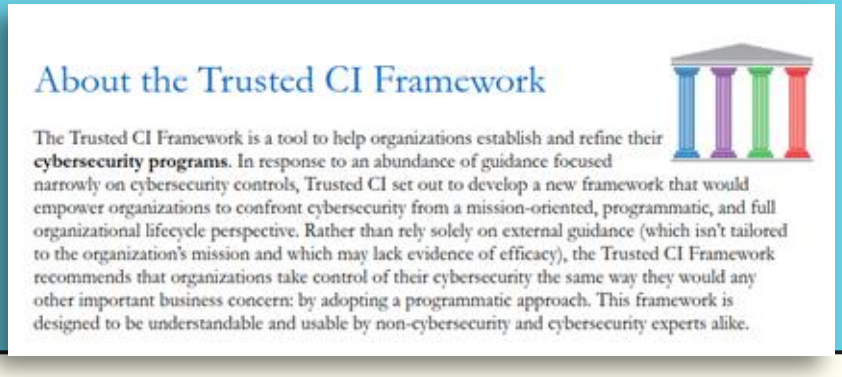


Security Exercises - Communication & Coordination

- Scope: LHC US Tier 2 sites for ATLAS and CMS
- Conducted a series of lightweight security exercises to validate secure comms
- Observed response patterns.
- Identified opportunities to improve
- Next exercise planned for 2H 2026

Future endeavors

- Continue existing vuln scanning, vulnerability curation and announcements
- Continue providing advice to rest of OSG team
- Facilitate more security exercises
- Evaluate OSG security program against the Trusted CI Framework



About the Trusted CI Framework

The Trusted CI Framework is a tool to help organizations establish and refine their **cybersecurity programs**. In response to an abundance of guidance focused narrowly on cybersecurity controls, Trusted CI set out to develop a new framework that would empower organizations to confront cybersecurity from a mission-oriented, programmatic, and full organizational lifecycle perspective. Rather than rely solely on external guidance (which isn't tailored to the organization's mission and which may lack evidence of efficacy), the Trusted CI Framework recommends that organizations take control of their cybersecurity the same way they would any other important business concern: by adopting a programmatic approach. This framework is designed to be understandable and usable by non-cybersecurity and cybersecurity experts alike.

The  Era

Current state of AI 

Capable of more advanced and automated attacks as well as discovering new vulnerabilities. Some that humans might not have discovered

Super AI ( s)

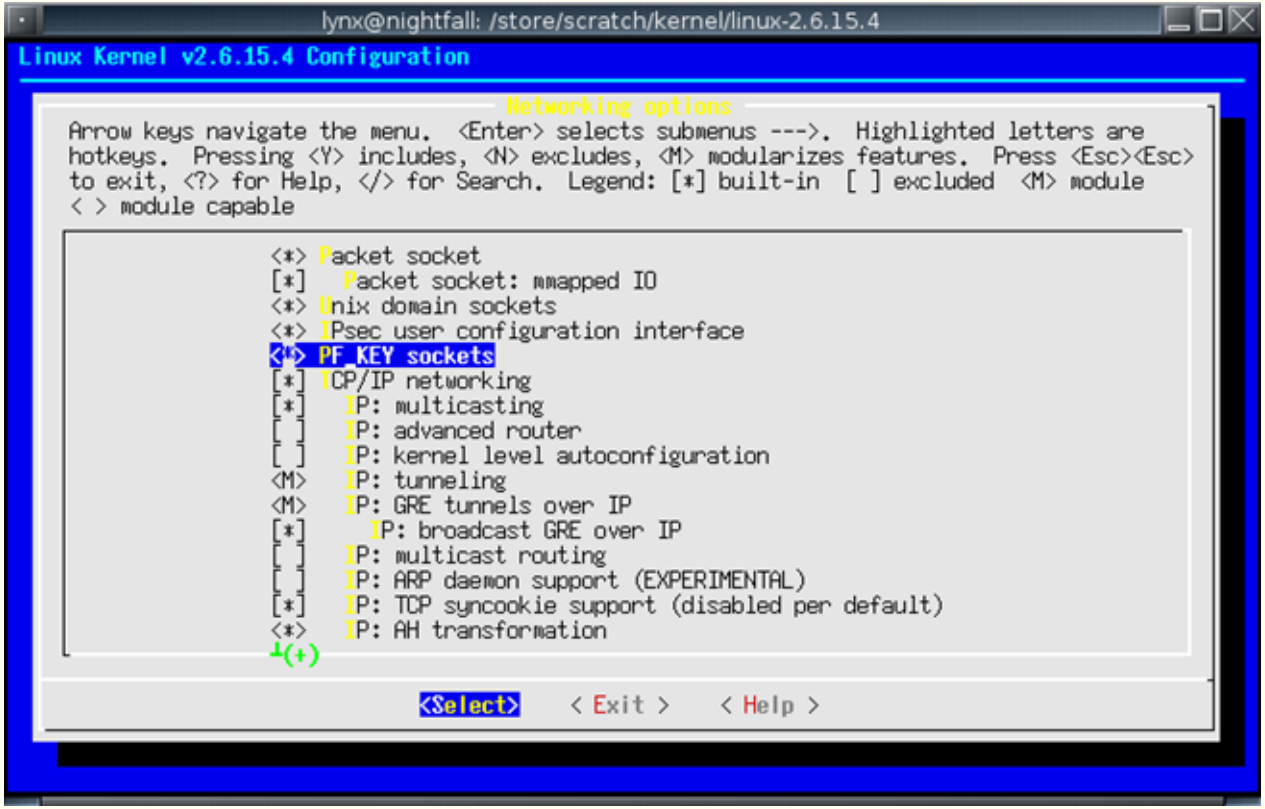
Reported to be capable of finding zero days within minutes. Could flood the community with more critical vulns than we can handle.

Typical remediation cycle

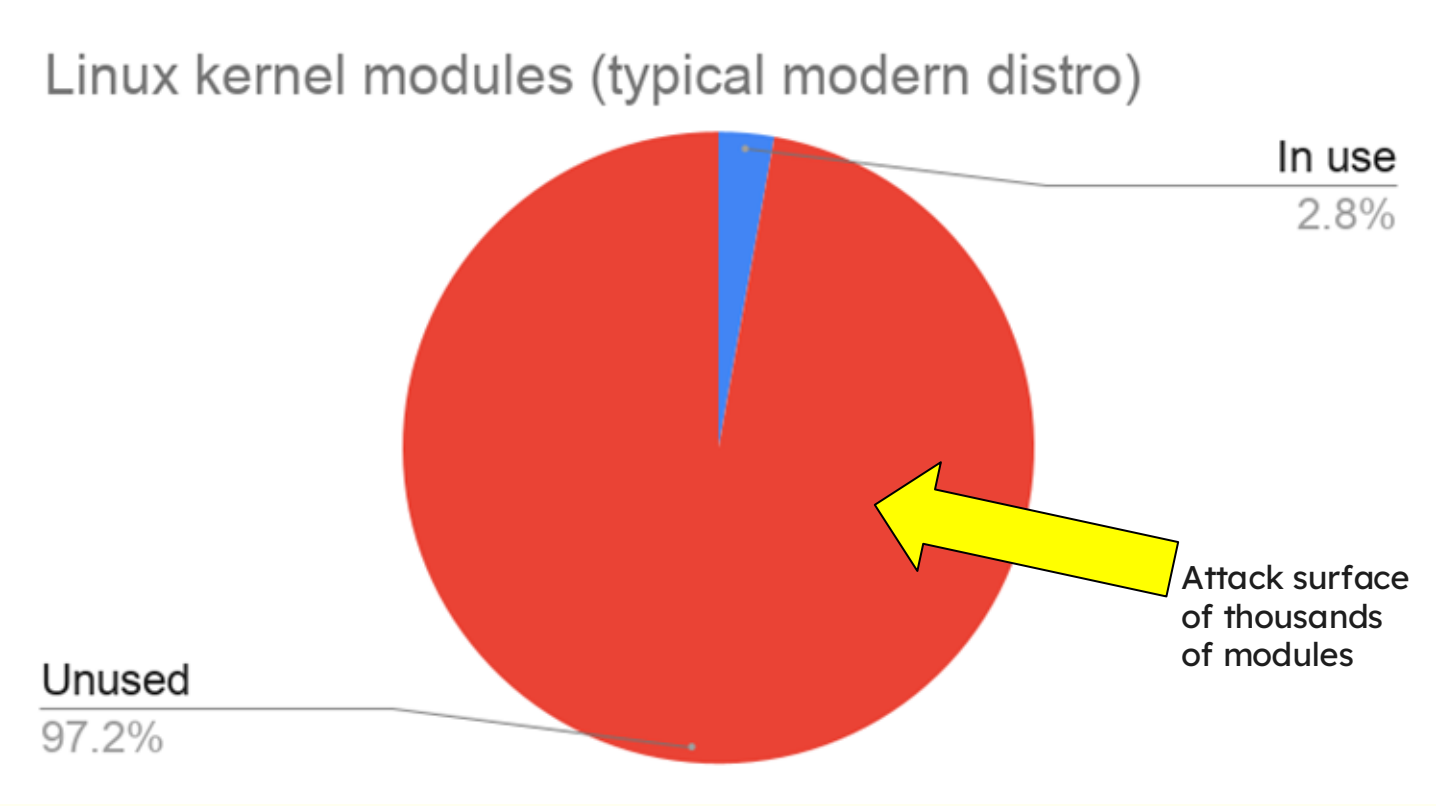
Kernel vuln patching usually requires a reboot = Downtime

Historical context to show how this risk has crept up on us.

Linux make config (old)



Kernel modules are attack surface



Default deny policy

About 95% of kernel modules go unused

That's a huge attack surface

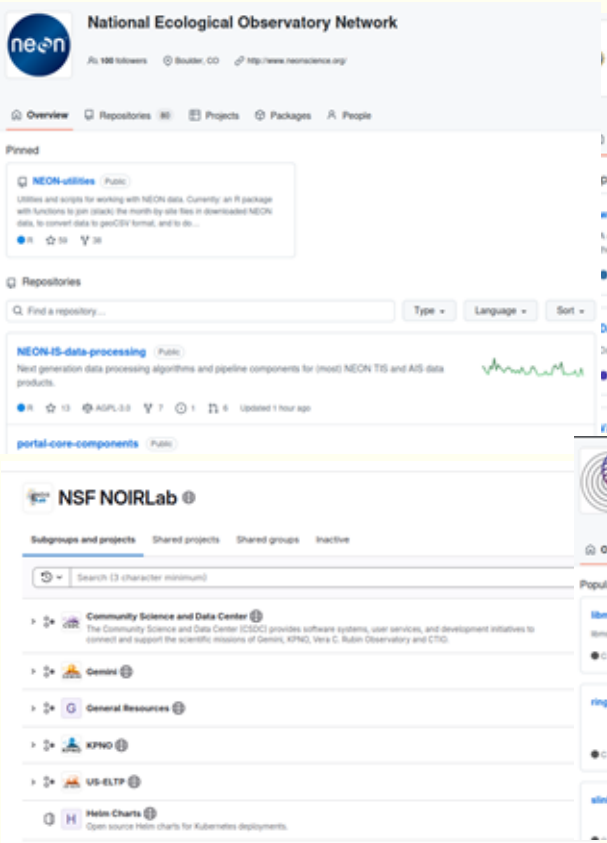
Maybe we could block them

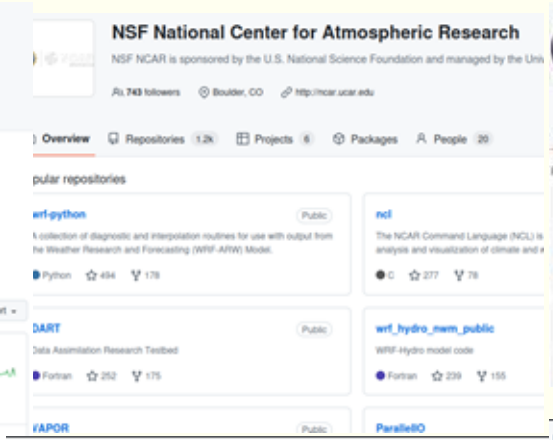
One and done config

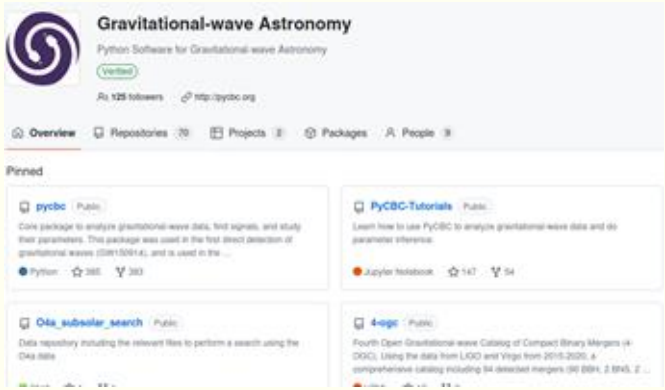
Tools that can be used

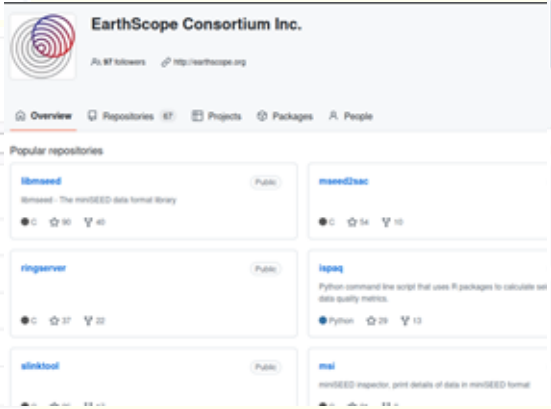
/etc/modprobe.d/*	ModuleJail	Modprobe-DB
• Text config files • Standard interface for controlling module loading • Once hardware and use cases are stabilized, it rarely changes • Saw recent use for DirtyFrag and CopyFail vulns	• https://github.com/jnuyens/modulejail/ • Shell script that scans running modules and denies the rest • Still requires one time curation	• https://github.com/grayskyy2/modprobed-db • Service that logs modules used during boot & runtime • Might catch some extra temporarily used modules

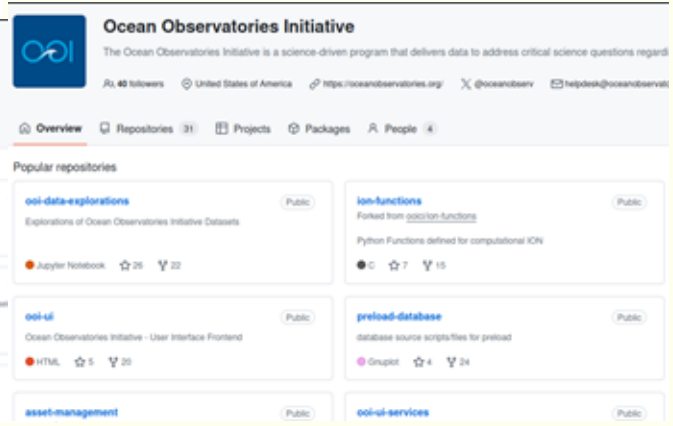
Bigger picture: Science at risk











Once in a generation risk

- Science projects deliberately expose a lot of code and data (ie. Github, downloads, datasets, etc.)
- AI-enabled vuln discovery may be pointed at science code
- Super AI ~~is on the horizon~~, which is maybe already here as of this week, is feared to find more as well as more complex vulnerabilities
- Similar to the challenge of Y2K
- Opportunity for NSF or government to step in and offer emergency response center for Science projects

Q&A

?