

June 11th 2026
Thursday

OSG Security Team



Because you're tired of hearing about AI

2



= AI

OSG Security Team

Mark Krenz

Adrian Crenshaw

Megha Moncy

Vishal Singh Bhardvaj

(Team members from IU)



Responsibilities

| | | |
|--|--|---|
| <p>Scanning for vulns</p> <p>Finding vulnerabilities relevant to the OSG consortium</p> <p>Weekly Nessus scanning of OSG-managed infrastructure</p> <p>~180 hosts monitored</p> <p>Coordination with service owners on remediation</p> | <p>Threat Intel</p> <p>Monitoring emerging threats and security advisories</p> <p>CVEs reviewed: 100+ per day</p> <p>Deep-dive analysis: 150+ (2025), 170+ (2026 YTD)</p> <p>Communications sent: 22 (2025), 43 (2026 YTD)</p> | <p>Community</p> <p>Supporting security discussions in Slack, Ops meetings, and PATH weekly meetings</p> <p>Security coordination with HTCondor, Pelican, LHC, and community services</p> <p>Helping teams understand risk and prioritize fixes</p> |
|--|--|---|



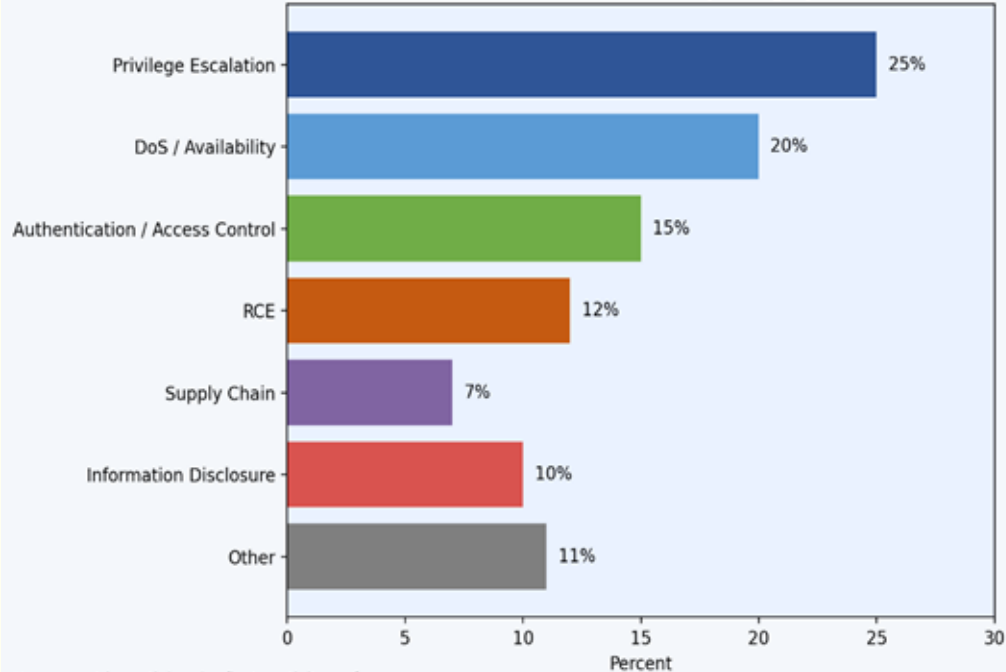
I DON'T ALWAYS WARN
ABOUT VULNERABILITIES

BUT WHEN I DO,
IT'S PRETTY BAD

Threat Intelligence Communication

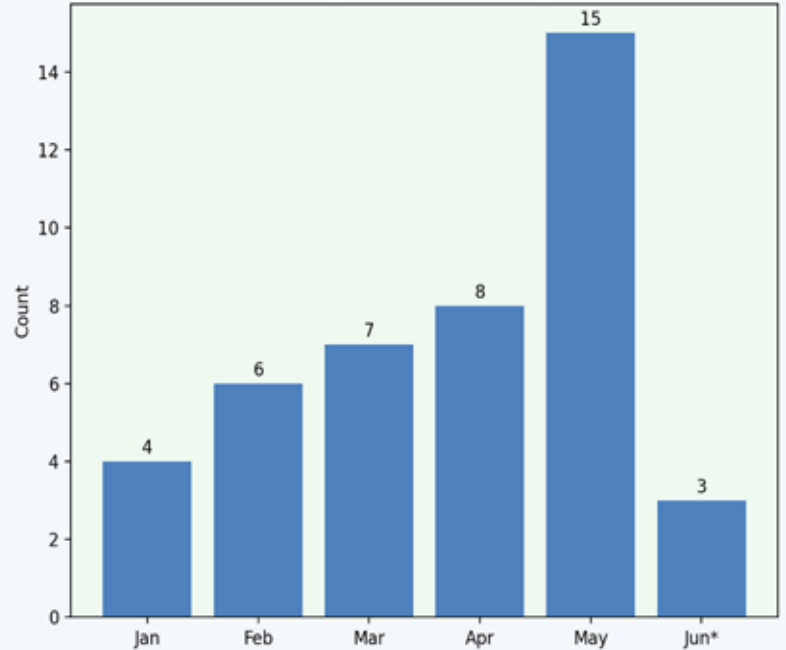
OSG Vulnerability Communications in 2026 (YTD)

Communicated Issues by Category



*June count is partial and reflects activity so far.

Community Communications by Month



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

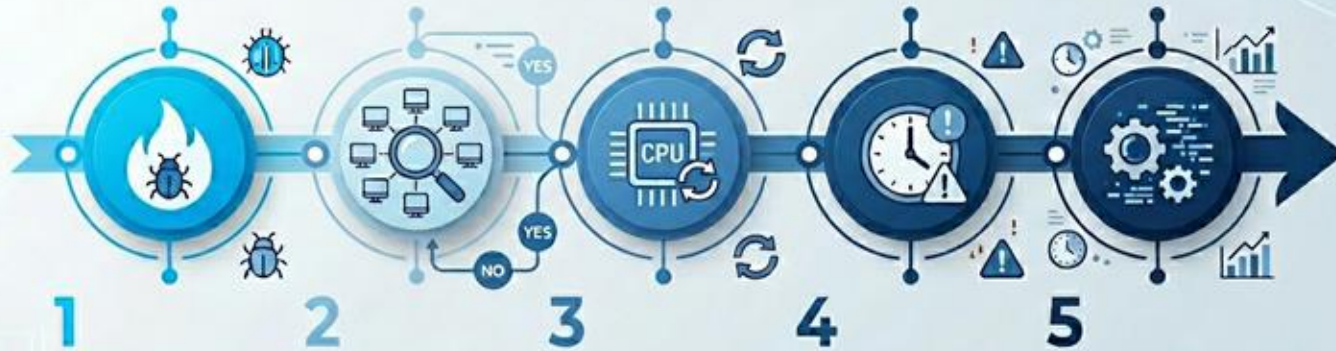
Capable of more advanced and automated attacks as well as discovering new vulnerabilities. Some that humans might not have discovered

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

Vulnerability Remediation Timeline



1
New CVE or exploit becomes public. Security researchers disclose a flaw.

2
Asset scanning & inventory check. Risk assessment of exposed systems.

3
Analyze vulnerability type. Determine if critical OS updates need a system restart.

4
Scheduling maintenance windows. Immediate patches and server restarts.

5
Interruption to research projects. Delayed experiments and scientific analysis.

Kernel vuln patching
usually requires a reboot
= Downtime

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

Linux make config (old)

```
lynx@nightfall: /store/scratch/kernel/linux-2.6.15.4
Linux Kernel v2.6.15.4 Configuration

Networking options
Arrow keys navigate the menu. <Enter> selects submenus --->. Highlighted letters are
hotkeys. Pressing <Y> includes, <N> excludes, <M> modularizes features. Press <Esc><Esc>
to exit, <?> for Help, </> for Search. Legend: [*] built-in [ ] excluded <M> module
< > module capable

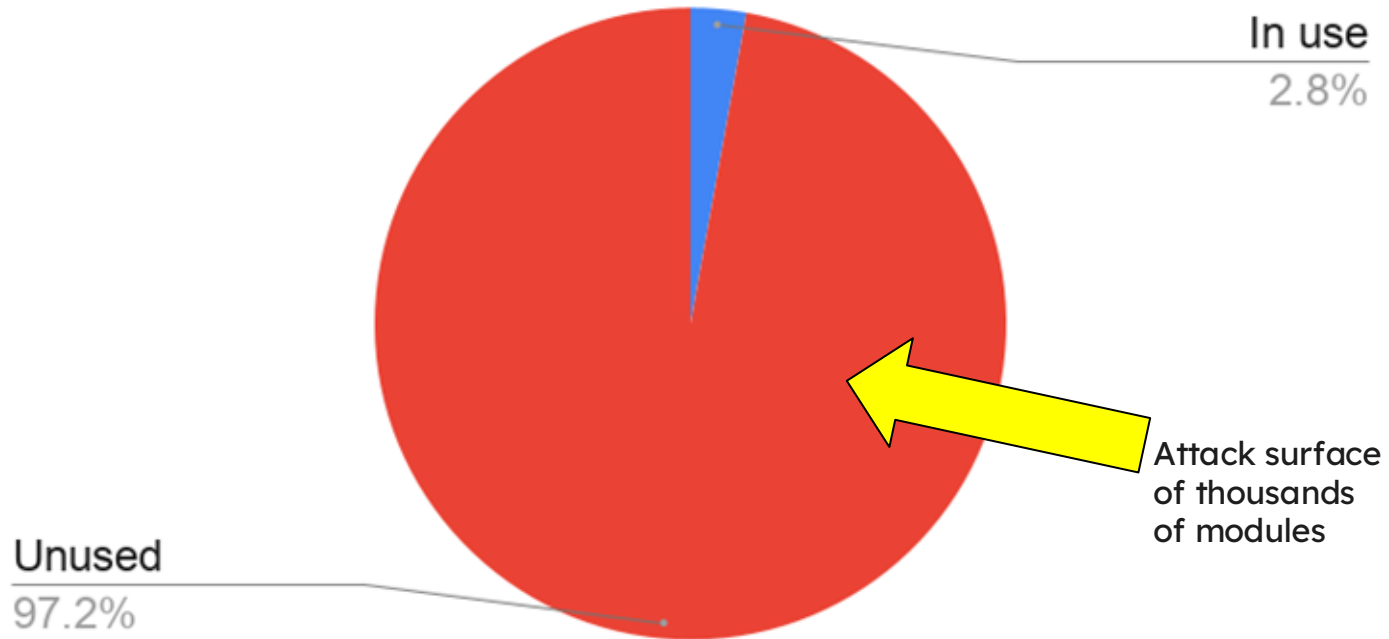
<*> Packet socket
[*] Packet socket: mapped IO
<*> Unix domain sockets
<*> IPsec user configuration interface
<*> PF_KEY sockets
[*] TCP/IP networking
[*] IP: multicasting
[ ] IP: advanced router
[ ] IP: kernel level autoconfiguration
<M> IP: tunneling
<M> IP: GRE tunnels over IP
[*] IP: broadcast GRE over IP
[ ] IP: multicast routing
[ ] IP: ARP daemon support (EXPERIMENTAL)
[*] IP: TCP syncookie support (disabled per default)
<*> IP: AH transformation
↓(+)
```

<Select> < Exit > < Help >

Kernel modules are attack surface

14

Linux kernel modules (typical modern distro)



Default deny policy

15

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

16

/etc/modprobe.d/*

- 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

ModuleJail

- <https://github.com/jnuyens/modulejail/>
- Shell script that scans running modules and denies the rest
- Still requires one time curation

Modprobe-DB

- <https://github.com/graysky2/modprobed-db>
- Service that logs modules used during boot & runtime
- Might catch some extra temporarily used modules

Bigger picture: Science at risk

17

The image displays a collage of GitHub organization profiles for several scientific research groups. Each profile includes the organization's name, logo, a brief description, and a list of popular repositories. The organizations shown are:

- National Ecological Observatory Network (NEON):** 188 followers, Boulder, CO. Pinned repository: `NEON-utilities` (Public).
- NSF National Center for Atmospheric Research (NSF NCAR):** 743 followers, Boulder, CO. Popular repositories include `erf-python`, `ncf`, `DART`, `wrf_hydro_mom_public`, and `fAPOR`.
- Gravitational-wave Astronomy:** Python Software for Gravitational-wave Astronomy. 125 followers, http://pycbc.org. Pinned repository: `pycbc` (Public).
- EarthScope Consortium Inc.:** 87 followers, http://earthscope.org. Popular repositories include `libmseed`, `ringserver`, `slinktool`, `libmseed2aac`, `ltaq`, and `msl`.
- Ocean Observatories Initiative:** The Ocean Observatories Initiative is a science-driven program that delivers data to address critical science questions regarding the ocean. 43 followers, United States of America, http://oceanobservatories.org. Popular repositories include `ooi-data-explorations`, `ooi-uf`, `asset-management`, `ion-functions`, `preload-database`, and `ooi-qi-services`.

Other visible repository titles include `NEON-IS-data-processing`, `portal-core-components`, `NSF NOIRLab`, `PyCBC-Tutorials`, `4-orig`, `ooi-subset_search`, `Community Science and Data Center`, `CentRI`, `General Resources`, `KPNO`, `US-ELTP`, and `Helix Charts`.

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

