

Homelabs

Craftsmanship in the Age of Vibe-Coded Everything

DEVOPSDAYS AUSTIN • MATTHEW BRAHMS



FOLLOW ALONG



scan to clone the demo repo

DEMO REPO

**git.brahms.cloud/matthew/
devops-days-austin-self-hosting**

Clone & follow the README · start early, model downloads
take a while

TALK NOTES

**md.brahms.cloud/
devops-days-austin-self-hosting**

Outline, resources, and links from today's talk



matthewbrahms



matthewbrahms




matthewbrahms





@matthewbrahms

About Me

 **Musician by trade**

 **I like to run**

 **Self-taught in tech**

 **Tech journey started when I moved to Austin**

Austin DevOps meetup at Rackspace is where it clicked



Where I Work

Platform engineer at Theori,
building Xint Code.


*You've probably seen us in the
news this week...*



THEORI

Xint

XINT CODE

 QUICK, DROP WHAT YOU'RE DOING AND READ

The most severe Linux threat to surface in years catches the world flat-footed

CopyFail threatens multi-tenant servers, CI/CD work flows, Kubernetes containers, and more.

DAN GOODIN - APR 30, 2026 3:20 PM |  160



→ Credit: Getty Images



Publicly released exploit code for an effectively unpatched vulnerability that gives root access to virtually all releases of Linux is setting off alarm bells as defenders scramble to ward off severe compromises inside data centers and on personal devices.

The vulnerability and exploit code that exploits it were released Wednesday evening by researchers from security firm [Theori](#), five weeks after privately disclosing it to the Linux kernel security team. The team patched the vulnerability in versions 7.0, 6.19.12, 6.18.12, 6.12.85, 6.6.137, 6.1.170, 5.15.204, and 5.10.254) but few of the Linux distributions had incorporated those fixes at the time the exploit was released.

A single script hacks all distros

The critical flaw, tracked as CVE-2026-31431 and the name CopyFail, is a local privilege escalation, a vulnerability class that allows unprivileged users to elevate themselves to administrators. CopyFail is particularly severe because it can be exploited with a single piece of exploit code—released in Wednesday’s disclosure—that works across all vulnerable distributions with no modification. With that, an attacker can, among other things, hack multi-tenant systems, break out of containers based on Kubernetes or other frameworks, and create malicious pull requests that pipe the exploit code through CI/CD work flows.

The Thesis

A homelab is a consequence-free production simulator.

It lets you practice ownership, constraints, failure, security, networking, storage, automation, and AI without waiting for permission.

Homelab vs. Self-Hosting

Homelab

Build things to understand them before they matter at work.

Self-Hosting

Run useful systems while reclaiming control of your data.

The Self-Hosting Manifesto



Self-sovereignty

You own your data. No rug-pulls. No en-crapification.



Hands-on with hardware

Build things. Break things. Learn how they actually work.



Find your community

Your people are out there. I guarantee it.

What Can You Self-Host?

Everything,

everywhere, all at once.

What I Self-Host Today

INFRASTRUCTURE

DNS
Reverse proxy
VPN / mesh
Ad blocking
OIDC
IP KVM
Monitoring
Alerting
Dashboard
Speedtest
SMART collection
Git forge + runners
Analytics
3 websites

MEDIA

Media server
IPTV
Photos
Music (4TB)
Audiobooks
Ebooks
Comics
YouTube Archive
YouTube Premium
Music history

PERSONAL

Documents
Recipes
Drive
Budget
RSS feeds
Notes sync
Weather station
Home automation
Location tracking
Car maintenance
Invoicing

MISCELLANEOUS

Matrix chat
Mumble
Remote desktop
Pastebin
Markdown collab
File converter
PDF Utility

AI

Local LLM chat
AI search
Voice assistant
Speech-to-text
Coding agents
Document RAG
Image enrichment
Recipe OCR

This Is Not Where You Start

**You start with the next
constraint.**

Mine was networking.

Homelab v1

ISP Modem



Netgear Nighthawk



24-Port TP-Link Managed Switch

Built from hardware companies
were disposing of.

- Domain controllers · Active Directory · Hyper-V
- Job-interview muscle memory
- Blockers: power, heat, noise



Then Kids Happened

8 years go by.

The Wrong First Assumption

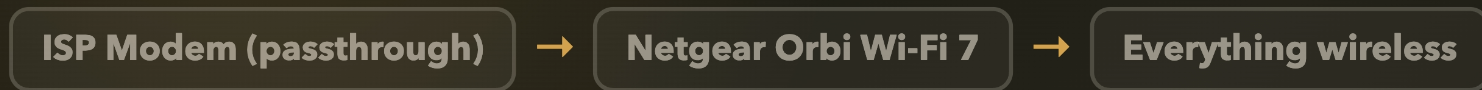
I thought I needed:

- More servers
- More disks
- More compute
- More GPU

What I actually needed first was a better foundation.

Networking: Problem

WHAT I HAD



WHAT WAS WRONG



WHAT WAS MISSING



Scope It Down

The decision was not "build a datacenter."

It was:

- 10GbE where it matters, not everywhere
- Wired AP backhaul
- VLAN isolation
- Secure remote access
- Reliable "enough" for family



Research Questions

- **Fiber or copper for 10GbE?**
- **Heat, power, and cost tradeoffs?**
- **What NICs work with old hosts?**
- **Can I use existing Cat5e?**
- **Is 10GbE only needed in the office?**
- **Can I install fiber myself?**
- **Does cutting holes void my builder's warranty?**
- **What are housing codes around fiber installation?**

OM4,5M/16FT*1Pack

- 🌡 Operating Temperature -20~70°C
- 🔗 LC/UPC to LC/UPC Connector
- 🔗 Physical Contact (upc)Connector
- 🌀 Support 1000BASE, 10GBASE, 40GBASE, 100GBASE
- 🛡 Maximum Protection
- 🔗 Mutil-mode Patch Cables
- 🌀 High Resistance to Micro-bending



Networking: Decision

Backbone

OM-4 fiber, pre-terminated cables + 100ft electrical conduit

10GbE scope

Office only – that's where the hardware lives

Platform

UniFi – not full Cisco, not OpenWRT. Practical, observable, job-adjacent

Self-install?

I can... but *should* I? 😬

The Bill of Materials

UniFi gear

UDM Pro Max · USW 10-port 10GbE Aggregation ·
USW Pro Max 24-port · Flex Mini 2.5G · Power
Distribution Pro

Cabling

OM-4 pre-terminated fiber cables · 100ft electrical
conduit

Build strategy

6 months · eBay used + new · DCA the spend



The Scary Part

01 20+ hours of fiber install videos

02 Fish rod acquired

03 Cut holes in my drywall

04 Crawled into the attic

05 Move ISP fiber line

😬 ...don't get caught!

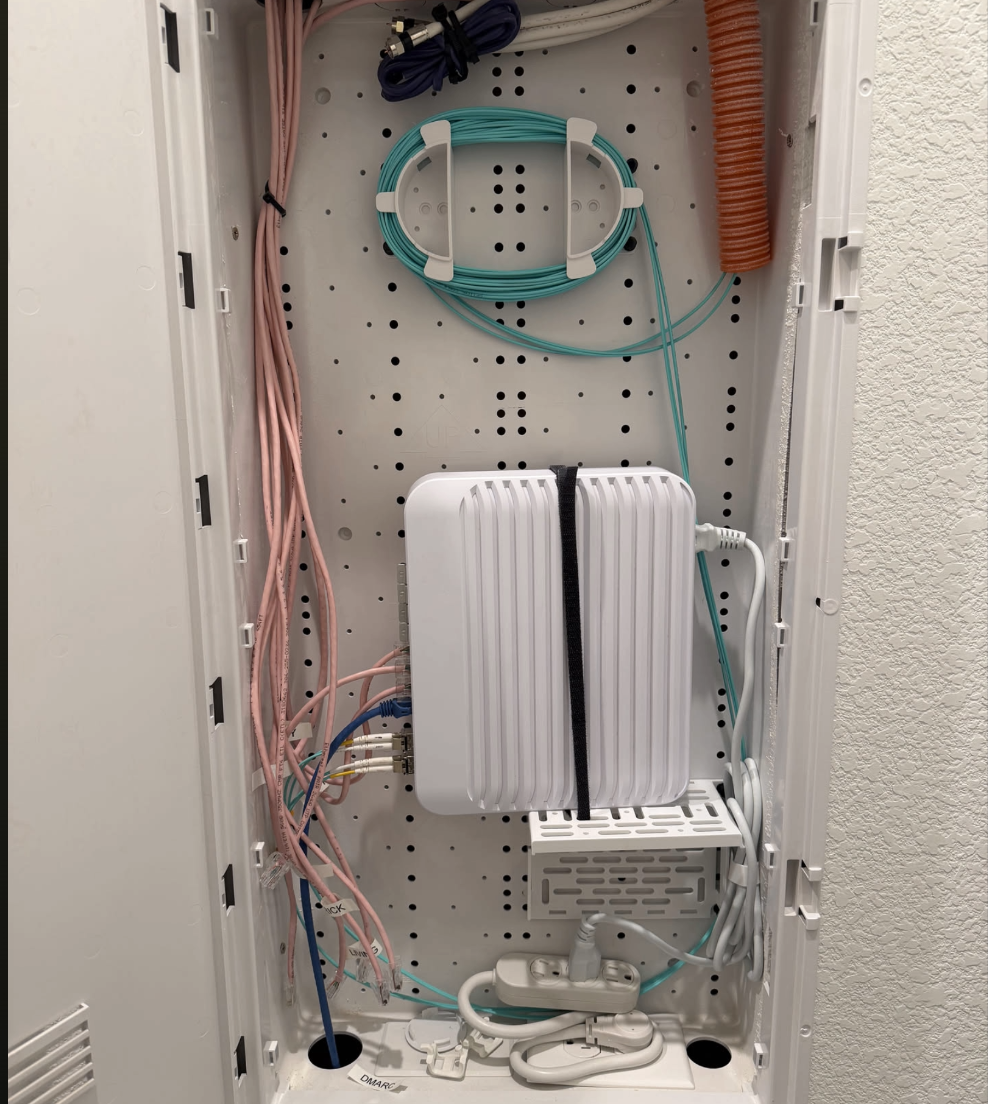






Execute The Build

- Pre-cut conduit
- Pull string through sections
- Unfurl OM-4 cables carefully
- Move direct-run fiber lines to utility box
- Drill hole in wall board
- Push both conduits down to drywall hole



Post-Op

The payoff was not just speed.

- ✓ **VLAN design practice**
- ✓ **AP management**
- ✓ **Secure remote access**
- ✓ **Better monitoring**
- ✓ **Real confidence from physical execution**



Hardware

Start with constraints, not wishlists.



A Word of Warning

**RAMpocalypse.
Storagepocalypse.**

**RAM and storage prices have spiked. Budget accordingly –
but don't let it stop you from starting.**

Three Hardware Archetypes

General Compute

DNS, monitoring, small services, general learning.

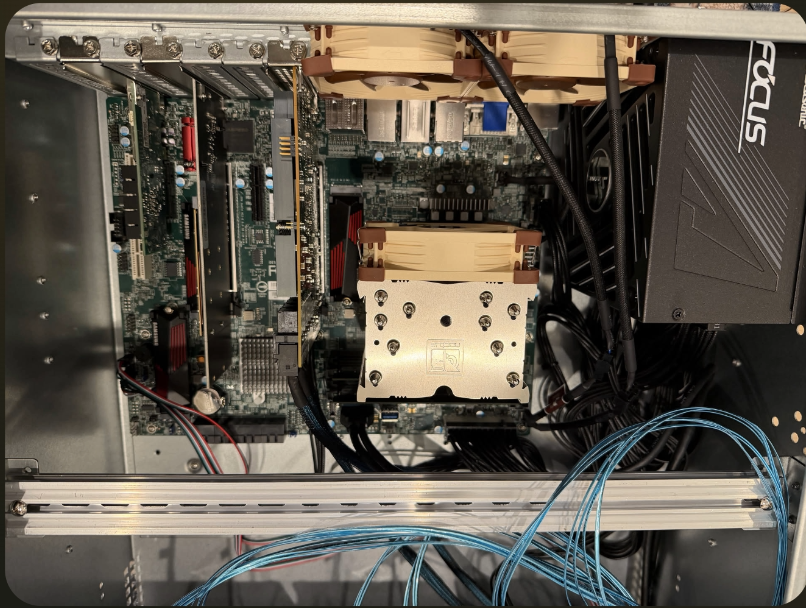
Media Server

ZFS, snapshots, media, photos, documents, backup reality.

GPU + AI

Local models, OCR, embeddings, image enrichment, coding agents.

Nixflix – The Media Server



CPU

Intel i5-14600K

RAM

64GB DDR5 ECC

Boot

2 × 1TB NVMe –
ZFS mirror

App data

2 × 4TB NVMe –
ZFS mirror via
bifurcation card

Scratch

4TB NVMe –
downloads & temp

Storage

10 × 20TB WD
SATA – two 5-disk
RAIDZ1 stripes
(~145TB usable)

OS

NixOS – running
63 containers,
declarative, rock-
solid

Storage Teaches Humility

Cloud hides storage nuances. At home, you go low-level fast.

- RAID is not backup
- Burn-in every drive – the bathtub curve is real
- ZFS snapshots are practical magic
- Backup strategy is not optional
- Capacity planning is a skill you actually develop



The Spinning Rust Details



Drives

10 × 20TB WD
SATA – two 5-disk
RAIDZ1 stripes

Usable

~182TB raw →
~145TB usable (2
parity disks)

Shucking

Pull bare drives
from WD external
enclosures –
cheaper than
buying bare

Buying strategy

Pairs over time;
different batches;
DCA over time

Burn-in

Thorough stress test
on every drive –
catch bathtub curve
failures early



Old Machines Still Work

🚫 You do not need a rack of enterprise servers

🖥️ 2 × i5-4430 desktops – 32GB DDR3, 750GB storage

🌐 DNS box: i5-2520M, 16GB DDR3 – sips power, never complains

★ Lenovo M720Q / M920Q – the sweet spot

~\$300-400 refurb · i5 · 32GB RAM · 500GB-1TB NVMe · tiny · cool · quiet

The GPU Server



CPU

Intel i9-9900K

RAM

64GB DDR4
Non-ECC

Storage

1TB NVMe –
boot & model
storage

GPU

NVIDIA RTX
4000 Ada –
20GB VRAM,
single slot

The GPU Is A Capability

Not the first purchase – but a transformative one.

- **RTX A4000** (16GB VRAM) – ~\$700-800 on eBay
- **RTX 4000 Ada** (20GB VRAM) – ~\$1,200 on eBay
- What it unlocks: local LLMs, document RAG, OCR, image enrichment, coding agents
- Can't afford it solo? **Go in with a friend, family member, or community**
- Share access over Tailscale – everyone benefits



Where Do You Find Hardware?

- **Start with what you have – old desktops, laptops, anything with a NIC**
- **eBay is the move – used/refurb is totally valid, don't buy new**
- **Give machines a second (or third) life – you'll be surprised what runs on a 10-year-old i5**
- **Lenovo M720Q / M920Q – best bang-for-buck small form factor on the market**
- **GPU hunt: eBay, r/hardwareswap, local Facebook Marketplace**
- **Only build when you need it – constraint drives creativity**

DevOps At Home

Rigor without cosplay.



My Tooling Arc

Chef and Puppet → Ansible → Terraform → Kubernetes → NixOS

The question is not which tool is best. The question is which failure modes you want to own.

The Home Production Rule

**Not everything needs to be
HA.**

**Some things just need to be understandable, recoverable,
backed up, and boring.**

What I Trust

- NixOS for base host state
- Docker Compose for app runtime
- Proxmox for general compute (LXC / VMs)
- ZFS for storage and snapshots
- Tailscale or mesh VPN for access

```
services.openssh = {  
  enable = true;  
  settings.PasswordAuthentication = false;  
};  
  
networking.firewall.enable = true;  
  
# that's it. jellyfin is running.  
services.jellyfin = {  
  enable = true;  
  openFirewall = true;  
};  
  
# docker too. no curl | bash required.  
virtualisation.docker = {  
  enable = true;  
  autoPrune.enable = true;  
};
```

Declarative Enough

```
services.ollama ≡ {  
  enable = true;  
  acceleration = "cuda";  
};  
  
virtualisation.oci-containers  
  .containers.open-webui ≡ {  
    image = "ghcr.io/open-webui/open-webui:main";  
    ports = [ "8080:8080" ];  
};
```

This is the same shape as the demo stack.

The progression is:

Docker Compose → repeatable
host → declared fleet

Self-Hosted AI

The laptop version first.



Demo Stack

Ollama

Local model runtime

Open WebUI

ChatGPT-like interface

SearXNG

Private metasearch

Perplexica

Perplexity-style search

Dockhand

Container visibility

OpenCode

Local coding assistant

Live Demo

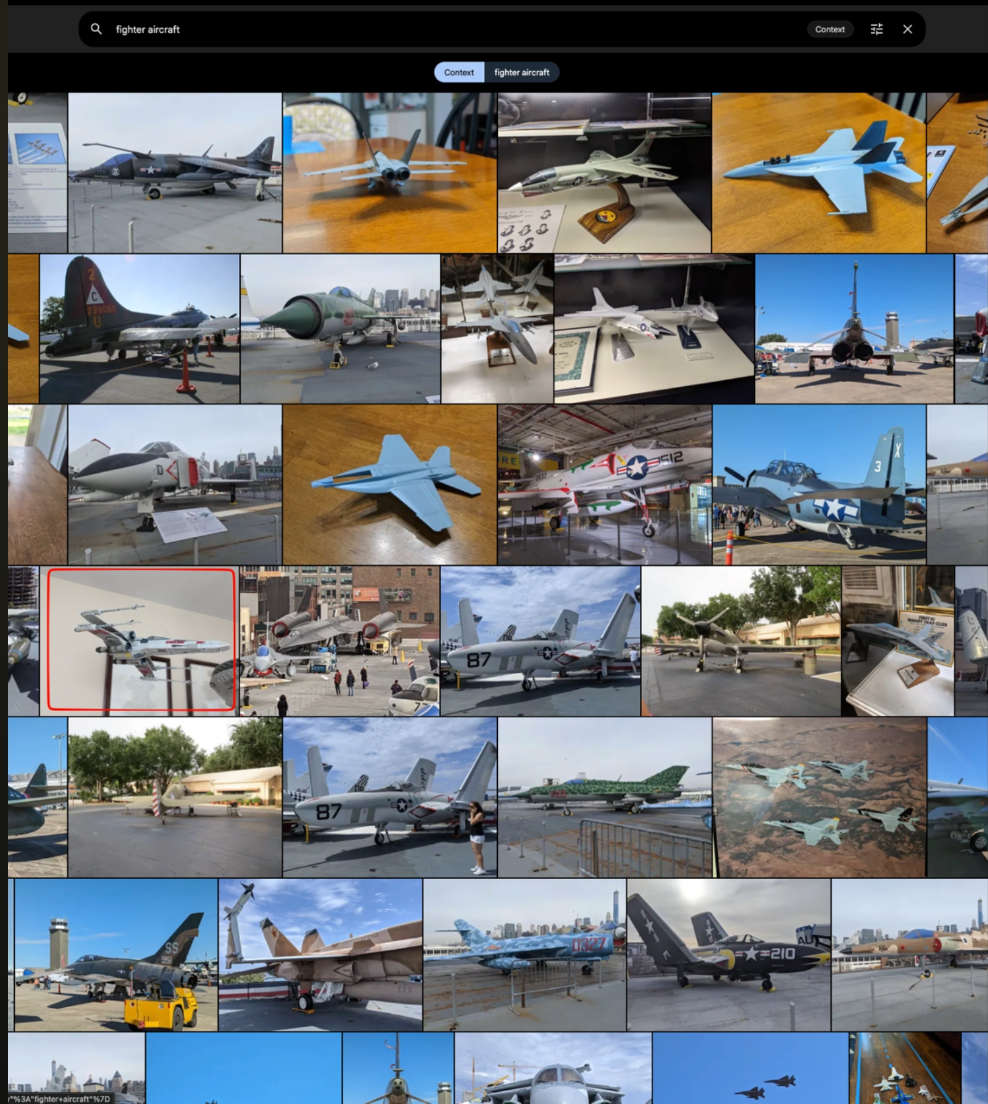
- 1. Dockhand: the stack is just containers**
- 2. Open WebUI: local chat**
- 3. Web search: local model + SearXNG**
- 4. OpenCode: local model in a developer workflow**

AI Becomes Useful At Home

Not as a toy.

As local capability:

- Photo enrichment
- Recipe OCR
- Document search
- Speech-to-text
- Coding support
- Family-accessible tools over mesh VPN



The Downsides Are Real

P1

OUTAGES

Your infra goes down. Your family notices. You get the ticket.

P2

BACKUPS

No SLA. No retention policy. No restore drill. Just you.

P2

SECURITY

Patch cadence, CVEs, exposed ports. You are the SOC.

P3

SUPPORT

"Why is Plex down?" is now a family support ticket at 9pm.

P3

COST

Hardware, power, bandwidth. The bill is yours to watch.

P4

COMPLEXITY

You chose this. Every layer you added is yours to maintain.

Next Iterations

3-2-1 Backup Execution

Turning backup theory into boring, tested restore paths.

Secrets For Agentic Use

Letting AI tools work safely without handing them the keys to everything.

3D Printing Infrastructure

Designing and printing the case for a dedicated backup NAS.

Agentic Homelab Skills

Building agents that can deploy, provision, and troubleshoot homelab infrastructure autonomously.

Build First Principles



Only build when you need it



Prefer used and refurb hardware



Start smaller than your ambition



Choose tools for their failure modes



Keep the restore path boring



Find your community

What To Build First

- 1** Whole-home ad blocking
- 2** DNS and DHCP you control
- 3** Photo hosting with a backup plan
- 4** Media server
- 5** Local AI chat
- 6** Monitoring for the machines you already have

Craft Still Matters

AI makes it easier to generate things. It does not remove the need to understand systems.

Build places where you can touch the whole stack, break things safely, and bring better judgment back to work.

AI brings some fear along with innovation. Let's experiment, build, and work as a community to level each other up!

Matthew Brahms

DEVOPS · PLATFORM ENGINEERING · SELF-HOSTER

DEMO REPO & SLIDES

git.brahms.cloud/matthew/devops-days-austin-self-hosting

Code, NixOS configs, and Docker Compose demo stack

TALK NOTES

md.brahms.cloud/devops-days-austin-self-hosting

Full outline, resources, and links from today



github.com/matthewbrahms



linkedin.com/in/matthewbrahms



x.com/matthewbrahms



techhub.social/@matthewbrahms