KubeCon CloudNativeCon North America 2026

#KubeCon #CloudNativeCon

AI Found a 0-Day in Metal3. What Happens Next?

Tuomo Tanskanen | Ericsson Software Technology



Who Am I

Tuomo Tanskanen

Principal Security Developer, Ericsson Software Technology (aka Ericsson Open Source)

Metal3 Core Maintainer and Security Committee Lead



tuminoid

tuomo.tanskanen@est.tech

Agenda

1. A Report Lands
2. Triage: What's Claimed and What's Real
3. From Valid Finding to Released Fix
4. When Your Upstream Has a Vulnerability
5. When We Release, Your Clock Starts
6. Pain Points, Roadmap, Takeaways

How a Vulnerability Disclosure Works



Sent privately to the security list. The clock starts.

Answer the reporter, form a Fix Team. Metal3 policy: 7 days. Triage pace follows the claimed severity.

Usually under embargo. Industry norm: up to 90 days.

Patch releases on supported branches, GitHub advisory, CVE.

The release starts the users' clock.

Every step has a deadline. The clock in the corner shows where we are.

Metal3 in 60 Seconds

Kubernetes Controllers	Packaged Upstream	Hardware
Cluster API Provider Metal3 (CAPM3)	ironic-image	BMCs: Redfish, vendor drivers, IPMI
Bare Metal Operator (BMO)	OpenStack Ironic	Boot: PXE, iPXE, virtual media
IP Address Manager (IPAM)	Ironic Python Agent	Firmware, BIOS and RAID settings
Ironic Standalone Operator (IrSO)		Provisioning network

T+0

Case: A Report Lands on the Metal3 Security List

Subject: Security issue in Cluster API Provider Metal3

Well structured and specific: file, function, code path

A plausible attack, with a PoC attached

A claimed severity, no affected versions

First impression: clearly from AI, and not obviously wrong

The Clock Starts

Day zero: a vulnerability nobody knew about, and no fix exists.

Policy: acknowledge the reporter within 7 days.

Claims High? Triage starts now.

Is it real?

KubeCon CloudNativeCon
North America 2026

T+0 + 1 min

The Reporter Was Me

In 2026, every Metal3 disclosure came from my own AI vulnerability discovery pipeline.

Before 2026: manual reports from outside researchers.



One Pipeline, Two Roles

The pipeline scans Metal3 and the OpenStack Ironic that Metal3 ships.

AI Vulnerability Discovery Pipeline

Metal3: I Am the Receiver

Findings go to the Metal3 Security Committee: our own process and schedule

OpenStack Ironic: I Am the Reporter

Findings go to the OpenStack security team; the fixes come back as bumps

Both projects triage every report as a team. My reports get no free pass.

Aside

Real Hardware Is Not Ephemeral

	Ephemeral VM	Real Server
Compromised	Delete and recreate	Firmware and BMC can persist across reprovisioning
Rebuild	Seconds	Tens of minutes per host: POST, firmware, disk wipe
Out of band	Hypervisor API	BMC: own OS, admin credentials, old crypto, vendor-paced fixes
Boot	Cloud image	Network boot: DHCP and PXE, unauthenticated by design
Testing a fix	CI spins it up	Ironic-level fixes need BMC emulation; most controller fixes do not
Rolling out	Rolling update	Maintenance windows, often air-gapped

KubeCon CloudNativeCon
North America 2026

T+0 - T+weeks

Vulnerability Disclosure Triage:
What's Claimed and What's Real?



T+days

Four Questions We Need to Ask

1 Is It Actually Real?

AI's PoC proves the code path, not the deployment.

2 Is It in Our Repo?

AI blames the nearest flaw, not the root cause.

3 Who Can Reach It?

AI loves preconditions worse than the attack.

4 How Bad, Really?

AI loves to over-hype severity.

A good report has:

Affected version range: does it cover every supported release?

File and line. A reproducer you ran, with its output.

The component and root cause named: Metal3, Ironic, a dependency or firmware.

A proposed patch. Even a wrong one shows where the fix belongs.

Preconditions: network position, role, credentials, configuration.

The exploit scenario, step by step.

The harm, or what the attacker gains beyond the preconditions.

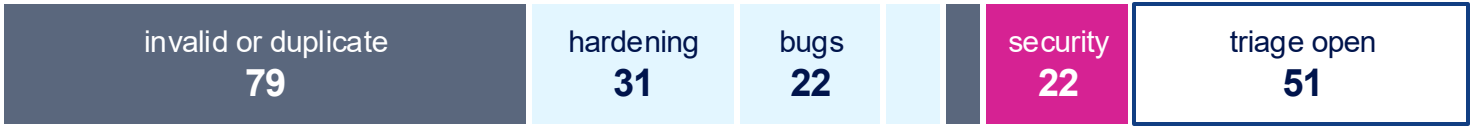
A CVSS vector, argued, not just a score.

A report that answers all four is actionable. In early 2026 ours did not. Today they do.

T+weeks

From Finding to Advisory

220 findings



9 by design, 6 cancelled

22 confirmed security issues

- **9** released in 4 advisories
- **13** disclosures in progress, on our own timeline

Discovery is fast. Fixing and coordinating is the slow part.

Metal3, 2026, from our triage tracker. Ironic findings go to the OpenStack security team.

KubeCon CloudNativeCon North America 2026

T+7d - T+90d

From Valid Finding to Released Fix



T+7d

Severity Decides the Path

Low

Private discussion first.

Then fixed in the open.

Ships when ready.

Medium

Private discussion first.

Then public PRs; security details stay private.

Coordinated to the next patch release.

High and Critical

Private fork until disclosure.

Out-of-band release.

Why low and medium go in the open: they are many, and mostly theoretical or hard to exploit. An embargo for each does not scale. The cost: the fix is public before the advisory.

Source: Metal3 security policy.

T+70d

The 0-Day: CAPM3 Cross-Namespace Access

Found	Triaged	First fix	Last variant	Backports	Released
03-09	03-18	04-16	04-23	04-29	05-18

Four Issues, CVSS 5.5, Fixed in the Open

Secret refs in Metal3Machine

BareMetalHost lookups via host annotation

ConsumerRef check used && instead of ||

Metal3DataTemplate refs from other namespaces

v1.13.0
all four fixes

v1.12.5
all four backported

v1.11.8
three of four: no v1beta2 webhook

Lesson learned: four issues in one advisory was a test, not to be repeated. One score and one fixed-version list cannot describe four bugs.

Release day

Four Advisories, One Release Day

Advisory	Component	CVSS	What	Fix on Main
GHSA-rf84-wr5g-m3rp	CAPM3	5.5	Cross-namespace access, four fixes	04-20 - 04-28
GHSA-49pm-43hf-6xfq	IPAM	4.4	Full CRUD on Secrets it never uses	03-25
GHSA-hfc8-w5f4-3x6m	IrSO	4.3	Labels user-owned Secrets	04-08
GHSA-7cwm-fpfh-rrch	IrSO	4.3	Metrics exporter on 0.0.0.0	04-17

The same rule, four times: medium and low, fixed in the open, advisories released together on 2026-05-18.

KubeCon CloudNativeCon North America 2026

Upstream clock

When Your Upstream Has a Vulnerability

Metal3 ships OpenStack Ironic.

The Metal3 Security Committee reported many of Ironic's 2026 advisories.

Every fix flows back to Metal3.





Upstream

The Bump That Came Back



A Security Fix in Disguise

ironic-image pins Ironic by git SHA digest per release branch.

The fix arrives looking like a routine Renovate bump.

Ironic, the Kubernetes Way

Standalone in containers, no Keystone, limited drivers.

Some advisories do not apply. Some depend on config, and Metal3's default config differs from upstream defaults.

Upstream

Reading an Ironic Advisory as a Metal3 User

Ironic Advisory

does not mean your Metal3 is vulnerable

No Metal3 Advisory

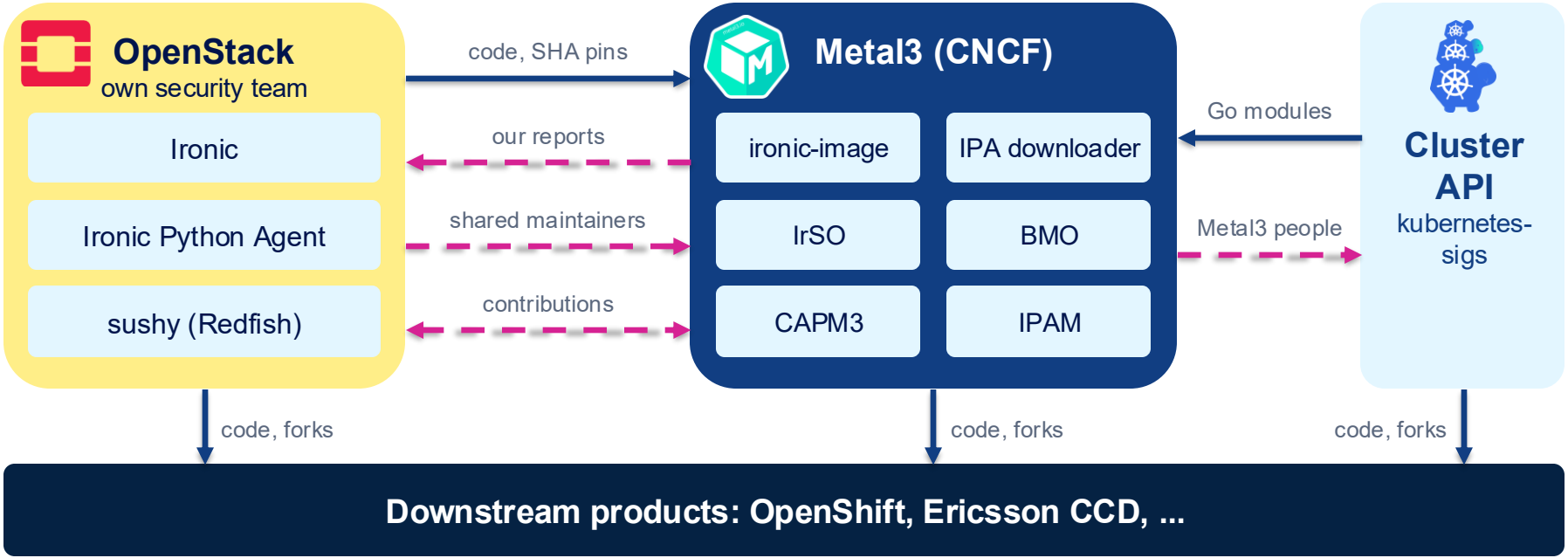
does not mean you are safe

Of the Ironic issues we disclosed, about 1 in 4 also affected Metal3.

Honest gap

The fixes ship in our releases: update and you have them. The announcement is missing. We do not yet alert Metal3 users to what an Ironic advisory means for them. That one is on us.

Upstream and Downstream at the Same Time



Solid: code. Dashed: reports and people.

KubeCon CloudNativeCon
North America 2026

T+release

When We Release, Your Clock Starts

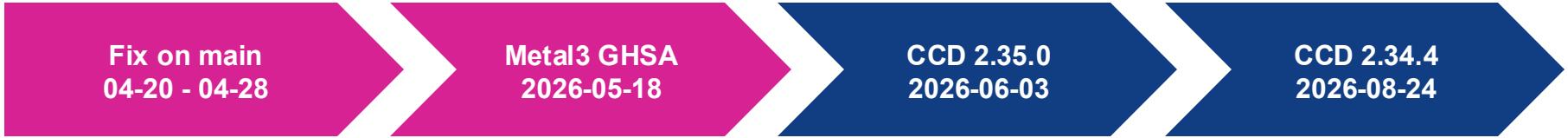
For everyone running Metal3



T+release

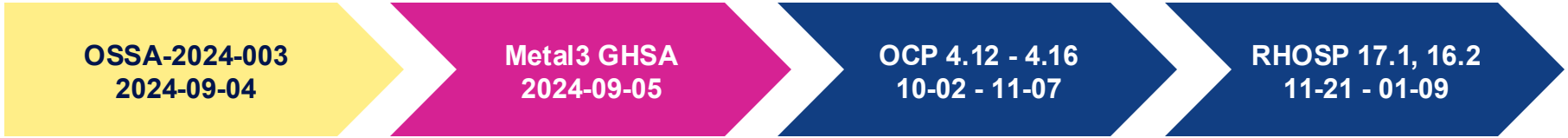
One Fix, Many Clocks

Metal3 to Ericsson CCD: GHSA-rf84-wr5g-m3rp (CAPM3, CVSS 5.5)



Both CCD releases ship CAPM3 v1.12.5, the backport.

Ironic to Metal3 to Red Hat: CVE-2024-44082 (qemu-img image data, CVSS 5.7)



Each hop runs its own clock and makes its own risk call.

T+release

Metal3 Guidance: How to Stay Safe

Run a Supported Release

The two latest stable releases get fixes.

One older release stays CI enabled, no patches except emergencies.

Main branch is under development.

Take the Latest Patch

Monthly patch releases for all controllers.

The latest patch of a supported branch carries every fix.

Watch releases on GitHub. A CVE scanner alerts once the advisory is out.

Know Your Configuration

Know what you have enabled, and why.

Follow the hardening guide. Check your settings against each advisory.

Fixed versions and workarounds for the 2026 advisories are in each GHSA.

T+release

Does It Affect You?

What we find most: multi-tenancy and role isolation, cluster-wide RBAC from the operator pattern, configuration combinations.

One Team per Cluster

CAPM3 is designed single-tenant: namespaces organise work, they do not isolate.

Some users share it anyway. That is why cross-namespace gaps get an advisory.

Most 2026 Metal3 findings: defence in depth.

Shared Cluster or BMaaS

BMO can be run multi-tenant, with per-namespace hosts and role isolation.

Several roles with different permissions raise the risk. Access is no longer all or nothing.

New features such as HostClaim get a multi-tenancy review from the design stage.

Our Pain Points and Roadmap

Pain Points

Versatile deployments, little visibility into how users run Metal3

Little hardening documentation

Upstream advisories are hard to translate for Metal3 users

Security fixes arrive as plain digest bumps

Fixes are public before the advisory; the window is too long

Backports to every supported branch; one fix could not reach 1.11

Roadmap

Hardening guide: in progress now

Streamline the internal report process

Streamline releases: shorter window from public fix to advisory, packaged upstream included

Analyse upstream advisories for Metal3 users: Ironic and every dependency

Help us: tell us how you run Metal3.

Three Things to Take Home

1. AI finds bugs fast, and not only for us. Shorten your upgrade cycle.
2. An advisory is not a verdict. Your configuration and tenancy decide if it affects you.
3. Using a distribution? Ask how fast Metal3 fixes reach you.

Tell us how you run Metal3: booth P-13B, Tue 10:30 AM-2:30 PM, Wed 10:15 AM-1:25 PM, Thu 10:15-11:55 AM



AI Found a 0-Day in Metal3. What Happens Next?

Session feedback

Thank you. Questions?

Found something? metal3-security@googlegroups.com

KubeCon CloudNativeCon North America 2026