EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 4 · 28 August 2026
Marcus Hale (PSIRT) · Tess Calder (red team) · Jessy Lang

That's Not a Zero-Day

Seven myths about the word, and the boring work that matters instead

"Zero-day" has become a word people reach for to create urgency, not to report a fact. It only says that exploitation began before the vendor could have known. It says nothing about severity or about whether you are exposed. The antidote was never a sharper alarm, but the work done long before one goes off.

MANUFACTURED URGENCY
Urgency made by a label, with no exposure beneath it.

1. Is this even a finding?

2. Did exploitation start before the vendor could know?

3. Is it being exploited, and does it matter to us?

MYTHS ABOUT THE WORD AND WHAT TO DO

1	**It says zero-day in the subject line** The word is a timestamp, not a severity.	Treat the label as a claim to check. Zero-day means exploitation began before the vendor had any opportunity to fix it. Ask whether it is exploitable and whether it is being exploited, before any label is attached.
2	**A decision reported as a vulnerability** A free-tier limit left soft on purpose was filed as a zero-day with a full CVSS breakdown.	Call the owner before you reply: is the behaviour intentional? A report resubmitted to a public tracker keeps its identifier, and somebody will cite it in a scan someday.
3	**An old N-day dressed as new** A technique with a CVE and a fix for eighteen months, relabelled zero-day.	Check the dates. If a CVE number and a fix existed before the exploit ran, the story is a gap in patch management that everyone could have prevented.
4	**A real zero-day that does not apply to you** The label told nobody whether they were exposed.	Exposure answers "should I be scared", the word cannot. Keep a written map of what each component touches and can reach. The client who had it isolated the integration within an hour.
5	**The boy who cried zero-day** After mostly noise, teams stop chasing alerts. Attackers count on it.	Do not stop reading past the subject line. Confirm real exploitation each time, because the tenth alert of the month is the one nobody staffs for.
6	**Someone is selling the panic** Bounty incentives, newsletters, leaderboards and push alerts all profit from the word.	Ask who benefits from the label and what is actually inside the box. Overclaiming has no matching penalty, and a quiet month is bad for engagement.
7	**The clock does not care** Under the CRA, notifying ENISA and the CSIRT starts at 24 hours from knowing of active exploitation.	Make triage mandatory: confirm exploitable and exploited before any label. That avoids starting a clock for noise and missing one for a real case.

WHAT WORKS INSTEAD

Threat-model the findings
Rank which findings can reach something that matters, fund the fixes, and defer the rest with a name and a reason.

Know what ruins your week
Ask which assets losing confidentiality, integrity or availability would hurt most, and spend the budget there.

Contain in advance
Segment where the crown jewels are, expire credentials on a schedule, and ask in advance what happens if one system is popped.

Listen to the episode
That's Not a Zero-Day and the rest of the series.
eacg.de
/en/podcast/s04-zero-day-mythos

Digital Product Design
From the first idea to a viable first release.
eacg.de
/en/consulting/digital-products

PSIRT Services
Intake, assess and disclose vulnerabilities, built or run as a service.
eacg.de
/en/consulting/psirt

© 2026 EACG GmbH