EACG
Enterprise Architecture Consulting Group

SECURITY DIALOGUES
No. 1 · 8 August 2026
Marcus (PSIRT) · Tess (incident response) · Jessy

Local or Network?

Seven reasons the network/local split fails, and three jobs it can still do

The proposal: split known vulnerabilities into network-exploitable and locally exploitable, with two clocks, an emergency response for the first and the ordinary patch cycle for the second. It fails in that form. The vector does not measure severity. It states a precondition, what an attacker must already hold, and a precondition only means something against a boundary you rely on.

BLAST RADIUS DEBT
The price of the first foothold.

1. What must the attacker already hold?

2. Which of my boundaries should prevent that?

3. Is it observed in the wild, or likely soon?

WHY THE SPLIT FAILS AND WHAT TO DO INSTEAD

1	**The vector is not the deployment** The same CVE is a nuisance on a laptop and a cluster compromise on a shared node.	Treat the base score as a starting point that expects revision, which is why environmental modifiers exist. A library's vector assumes a reference use: your product may expose the path over an API, compile it out or never call it.
2	**Network is not internet** "Network exploitable" is heard as "reachable from the internet".	Vector is not exposure, so ask the two questions separately. An internal-only service still scores as network. The converse bites as well: internet-facing but only locally exploitable gets filed as calm.
3	**The middle disappears** A binary throws away adjacent and physical.	Keep them in view. In operational technology the adjacent bus is the threat model; in automotive a physical connector is within reach. For anything you ship into someone else's hands (a meter, a set-top box, a vehicle, a payment terminal, a games console) local is the attacker's starting condition, and the network they need is a screwdriver.
4	**Local does not mean prior compromise** Build runners, containers, hypervisors, sandboxes and kernels are boundaries we depend on.	Pair the vector with the trust boundary. Three classes: no prior position needed (the emergency class); a position that a boundary you depend on should deny (container escape on shared infrastructure, multi-tenant hosts, build runners, devices the customer holds), which is nominally local and operationally identical; a position that grants nothing you had not conceded, which can wait.
5	**Attacks are chains** Local is the second to fifth link of nearly every intrusion.	Do not prioritise only the door. Escalation, credential theft from memory and container escape are all local. Attackers do not decline a vulnerability because it scored lower, and a substantial share of the lists of vulnerabilities observed in the wild are local escalations.
6	**An advertised window** Two published clocks tell every adversary how long they have.	Do not publish a patch cadence that parks a class of vulnerability for ninety days. Declaring it second-tier does not make it less dangerous, it makes it more attractive, because you have guaranteed its availability.
7	**The vendor ranks for the operator** The ranking is a fact about the operator's architecture.	The vendor states the precondition precisely: what an attacker must hold, which configurations are affected and which are not, machine-readable if possible. The operator, who alone knows the architecture, does the ranking. The priority is the intersection.

THREE JOBS THE DISTINCTION KEEPS

Language, never a closer
"Requires local access" tells a customer something true and useful. Use it as context, not as reassurance, and never to end the conversation.

One input among three
Observed in the wild overrides everything. Probability of near-term exploitation tilts the order within a bucket. The vector supplies the precondition. None works alone.

Measure blast radius debt
Track the size of the locally-exploitable backlog on systems where a boundary depends on it. It shows how expensive the first breach would be.

Listen to the episode
Local or Network? and the rest of the series.
eacg.de
/en/podcast/s01-net-vs-local

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